Pekka Riisalo

Windows-palvelinympäristön virtuaalisointi

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

20.6.2014

Metropolia

Tekijä Otsikko Sivumäärä Aika	Pekka Riisalo Windows-palvelinympäristön virtuaalisointi 31 sivua 9.6.2014
Tutkinto	insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Sulautettu tietotekniikka
Ohjaaja	yliopettaja, Matti Puska

Insinöörityön aiheena on palvelinympäristön virtuaalisointi. Päämääränä projektissa oli toteuttaa kuvitellun yrityksen palvelinympäristö kotikäyttöisellä PC:llä. Itse PC toimii isäntäkoneena yhdelle tai useammalle palvelimelle, jotka toteutetaan virtuaalisesti. Insinöörityön painopiste keskittyy palvelinverkon rakentamiseen, ja siksi kaikkia sen toimintaperiaatteita ei käydä läpi. Itse projektia ei ole tarkoitus soveltaa missään, joten pääpaino on uusien asioiden oppimisella. Projektin olisi tarkoitus syventää hankittua tietämystä yrityksen IT-infrastruktuurin rakentamisesta ja ylläpidosta.

Isäntäkoneessa käyttöjärjestelmänä toimii Windows 7, ja sen resurssit jaetaan sen itsensä lisäksi kaikille virtuaalikoneille, joten varsinkin muistin (8 GB) määrä on rajallinen. Kahdella virtuaalikoneella on kuitenkin mahdollista toteuttaa kaikki tarvittavat tilanteet, kun asentaa useamman roolin samalle koneelle. Virtuaalisointi toteutetaan WMware Workstation 10-ohjelmistolla, joka on sarjan uusin tuotos. Palvelimien käyttöjärjestelmänä toimii Windows Server 2012 R2, joka sekin on uusinta teknologiaa. Projektin olisi voinut toteuttaa kevyemmillä ohjelmistoilla, mutta Windowsin käytön yleisyys vastaavissa järjestelmissä on niin suuri, että siihen kannattaa perehtyä.

Palvelinympäristön toteutus onnistui kokonaisuudessaan hyvin. Kahdelle virtuaaliselle palvelimelle saatiin asennettua mm. ADDS-, SQL-, VPN- ja Web-palvelimien roolit. Ainoastaan Exchange-sähköpostipalvelin, joka yksin vaatii 8 GB muistia, oli mahdoton toteuttaa käytössä olevilla työkaluilla. Asennuksen jälkeen käyttöjärjestelmä hidastui siinä määrin, ettei palvelin saanut enää käskyjä suoritettua.

Virtuaalisoimalla saa helposti aikaan testiympäristön, jossa voi kokeilla erilaisia kokoonpanoja ilman riskejä. Se on myös olennainen työkalu palvelinverkon rakennuksessa. RAID-tekniikkaa apuna käyttäen saadaan useista yksittäisistä koneista yhdistettyä suuria kokonaisuuksia, joissa resurssien ja tallennustilan jakaminen on yksinkertaista.

Avainsanat	virtuaalisointi, Windows, palvelin

Author Title Number of Pages Date	Pekka Riisalo Virtualizing Windows server environment 31 pages 9 June 2014
Degree	Bachelor of Engineering
Degree Programme	Information technology
Specialisation option	Embedded systems
Instructor	Matti Puska, Principal Lecturer

The subject of this thesis is virtualization of server environment. The project included building a server network of an imaginative corporation by using virtualization on a home PC. The main goal in the project was to gain deeper knowledge of how things work in a regular server network. This project is about building the default server network with the roles usually needed, and therefore some features of servers and applications are skipped. The project is done for learning purposes only.

The host computer is a PC running Windows 7. The resources of PC are spread among itself and multiple virtual servers, which can make adding some server roles difficult. However, every required task can be simulated using two virtual servers simultaneously. Memory pool of 8GB was thought to be enough for most roles. Virtual servers were made using WMware Workstation 10 and virtual server are using Windows Server 2012 R2.

Most of the planned roles were able to work in the environment, but Exchange mail server required all 8GB by itself. Installation was successful but afterwards the server could no longer be operated being so slow. VPN - and SQL servers provided some challenge, but a big part of installations were automatic or well instructed.

Virtualization can provide a great test environment and it is also a key tool in building large server networks. Used together with RAID, virtualizing can build huge entities with easy and versatile resource sharing.

Keywords	virtualization, Windows, server

Sisällys

Lyhenteet

AD	*Active Directory*. Vanha nimitys ADDS:lle.
ADAC	*Active Directory Administrative Center*. AD:n työkalu, jolla voidaan muokata AD:ssa sijaitsevia tietueita.
ADDS	*Active Directory Domain Services*. Ohjelmisto, jolla hallitaan käyttäjätilejä, konetilejä sekä erilaisia käyttäjäryhmiä.
DC	*Domain Controller*. Verkkoa hallitseva keskuspalvelin johon muut palvelimet kytkeytyvät.
DDoS	*Distributed Denial of Service*. Hyökkäys palvelinkonetta vastaan, missä ylikuormitetaan palvelinta käyttämällä palvelimen tarjoamia palveluita samanaikaisesti usein tuhansilla kaapatuilla koneilla.
DHCP	*Dynamic Host Configuration Protocol.* Protokolla, joka jakaa automaattisesti verkkoasetukset verkkoon liittyvälle laitteelle.
DNS	*Domain Name Server*. Palvelin, joka muuttaa nimet IP-osoitteiksi.
IIS	*Internet Information Services*. Palvelu, joka välittää informaatiota Internetiin ja takaisin päin.
IP	*Internet Protocol*. Protokolla, jolla koneet ottavat toisiinsa yhteyttä verkon yli.
ISP	*Internet Service Provider*. Verkon Internetin palveluntarjoaja.
LAN	*Local Area Network*. Lähiverkko, joka on rajoitetulla maantieteellisellä alueella toimiva tietoliikenneverkko
RAID	*Redundant Array of Independent Disks*. Teknologia, jonka avulla voi yhdistää useampia levyjä yhdeksi suuremmaksi kokonaisuudeksi.

RDP	*Remote Desktop Protocol*. Microsoftin kehittämä protokolla verkon sisällä tapahtuvaan etäkäyttöön.
SCCM	*System Center Configuration Manager*. AD:n vierellä toimiva ohjelmisto, jolla voidaan hallita yksittäisiä työasemia muuttamalla asetuksia tai asentamalla ohjelmia ja päivityksiä.
SQL	*Structured Query Language*. Ohjelmointikieli, jolla voi luoda tietokantoja sekä niitä käyttäviä kyselyitä.
UPS	*Uninterruptible Power Supply.* Virtalähde, joka tasoittaa virran kulkua poistaen virtapiikit ja keräten samalla jännitettä itseensä sähkökatkoksen varalle.
WAN	*Wide Area Network*. Laajaverkko, joka yhdistää lähiverkot ja kaupunkiverkot yhdeksi kokonaisuudeksi.
VPN	*Virtual Private Network*. Internet yhteyttä hyväksi käyttäen luodaan suora yhteys kotiverkkoon.

1 Johdanto

Lähes jokainen yritys vaatii nykyään paljon tietotekniikkaa pystyäkseen vastaamaan modernin markkinatalouden asettamiin haasteisiin. Ilman verkkosivuja ja hienoa IT-infrastruktuuria toimivaa yritystä ei enää oteta missään vakavasti. Tämä vaatii yritykseltä paljon työtä ja osaamista tai vähintäänkin tietoteknisten ratkaisuiden ulkoistamista. Usein päädytäänkin juuri ulkoistamaan palvelimet sekä niiden ylläpito jollekin alan monista yrityksistä. Kyseiset yritykset panostavat palvelinkeskuksiin, jotka muodostuvat suurista määristä tehokkaita ja paljon tallennustilaa tarjoavista tietokoneista. Teho ja tallennustila harvoin kuitenkin vastaavat täydellisesti yrityksen tarpeita yksittäisessä koneessa. Esimerkiksi kukkakaupan verkkokauppa ei välttämättä vaadi omaa fyysistä palvelinta palveluntarjoajalta. Virtualisoimalla useita palvelimia yhdelle tietokoneelle saadaan jaettua yhden fyysisen koneen resurssit usean asiakkaan käyttöön. Jotkin palvelimet tarvitsevat myös roolinsa vuoksi oman käyttöjärjestelmänsä. Lisäksi tietokoneiden tallennustila ja nopeus kasvavat paljon nopeammin kuin palvelinten vaatimat resurssit. Tästäkin voisi jo päätellä, että virtuaalisoinnin merkitys palvelinympäristöissä tulee ainoastaan kasvamaan tulevaisuudessa.

Insinöörityön aiheena on kuvitteellisen yrityksen palvelinympäristön virtuaalisointi. Viettämällä yli puoli vuotta erilaisissa lähitukitehtävissä sai kokemusta yrityksen palvelinympäristön toiminnasta. Kokemusta voi kuitenkin kuvailla parhaimmillaankin vain pintaraapaisuksi, eikä mahdollisuutta ollut päästä käsiksi syvempään tietämykseen työtehtävien puolesta. Halusin tietää asiasta enemmän, ja päädyin tekemään aiheesta insinöörityötä. Koska oikean verkon rakentaminen vaatii liikaa resursseja, päädyin rakentamaan mahdollisimman tarkan simulaation kuvitteellisen yrityksen palvelinverkon rungosta yhdellä koneella virtuaalisointia hyväksi käyttäen. Koko projektin ideana on siis rakentaa simuloitu versio minkä tahansa yrityksen palvelinympäristöstä pienemmässä mittakaavassa. Periaatteessa siis samalla tavalla palvelinympäristön voisi alustaa suureenkin yritykseen levytilaa ja kaistaa lisäämällä.

Yksi haaste palvelinten virtuaalisoinnissa on rajapinnan toteuttaminen siten, että sen käyttäminen myös isäntäkoneen ulkopuolelta onnistuisi kuten samassa verkossa olevien fyysisten palvelinten käyttäminen. Kirjautumisen palvelimelle pitäisi vaatia mahdollisimman vähän muutoksia mille tahansa fyysiselle koneelle, joka liitetään

verkkoon kytkimen avulla. Alan uusimmat ohjelmistot pystyvät virtualisoimaan palvelinten käyttöjärjestelmien lisäksi myös niiden verkkoympäristön. Käyttötarkoituksen mukaan voi valita, millä tavalla palvelimet on ”kytketty” isäntäkoneeseen tai sen verkkoon.

Kokonaisuuteen on tarkoitus liittää käyttäjän hallinta, työasemien hallinta, verkkolevyt, sähköpostipalvelin sekä etäkäyttömahdollisuus. Käyttäjiä sekä konetilejä hallinnoidaan toimialueen hakemistopalvelua käyttämällä, sähköpostin toimintaa hallinnoi erillinen sähköpostipalvelin ja työasemia pystytään hallinnoimaan hakemistopalvelun, sekä järjestelmänhallintaohjelmiston avulla. Virtual Private Networkin (VPN) kautta verkkoon pääsee käsiksi mistä tahansa internet yhteyden avulla, ja verkossa palvelimia voi hallita Remote Desktop-toiminnolla. Projekti toteutetaan yhdelle tai useammalle virtuaaliselle palvelimelle. Kaikki pyritään toteuttamaan yhdellä kotikäyttöön suunnitellulla Windows 7 -käyttöjärjestelmällä toimivalla käyttöpäätteellä.

2 Palvelinten rooli yrityksessä

2.1 Vastuu palvelinten toiminnasta

Palvelimien toiminnan merkitystä ei voi liiaksi korostaa yrityksen kannalta. Kaikki tieto liikkuu palvelinten kautta, eikä mitään tapahdu ilman että tieto liikkuu ihmisten välillä. Sähköpostit, verkkolevyillä olevat dokumentit, puhelinjärjestelmät, pikaviestimet, internetyhteys ja muutkin tietoa käyttävät ja välittävät palvelut vaativat palvelimilta moitteetonta toimintaa. Tämän takia ylläpitäjällä on todella suuri vastuu yrityksen toiminnassa.

Palvelinten ylläpito vaatii asiantuntemusta sekä paljon muita resursseja. Nämä syyt houkuttelevatkin yrityksiä ulkoistamaan palvelimensa jollekin alan yritykselle, jolla on enemmän tietämystä ongelmatilanteista ja varakoneita laiteongelmien ilmetessä. Palvelinpalveluita tarjoava yritys ei myöskään tarvitse yhtä monta asiantuntijaa järjestelmää kohden kuin mahdollinen asiakas. Useampaa järjestelmää ylläpitäessä pieniä ongelmia ilmenee useammin, mutta oletettavasti kriittisiä tilanteita ei koskaan ole kaikilla samaan aikaan. Näin pienempi määrä asiantuntijoita pystytään jakamaan suuremmalle määrälle yrityksiä. Myös fyysiset koneet vaativat omat

erikoisjärjestelynsä. Nämä olosuhteet ja varajärjestelmät on suhteessa edullisempi luoda suurelle määrälle koneita kerrallaan. Edellä mainitut seikat mahdollistavat palveluiden hinnoittelun sille tasolle, että joidenkin yritysten kannattaa niitä käyttää. Myös palvelinverkon toimintavarmuus on yleensä parempi ulkoistettuna hyvin toimivalle palveluntarjoajalle. Ulkoistamisessa on kuitenkin aina omat ongelmansa. Informaation välitys yritykseltä toiselle on aina mutkikkaampaa kuin yrityksen sisällä tapahtuva kommunikointi. Täytyy tarkkaan määrittää, minkälaiset ongelmat voidaan antaa oman yrityksen ulkopuolelle ratkaistavaksi, ja sääntöjen määrä heikentää aina yrityksen kykyä toimia joustavasti yllättävissä tilanteissa. Palvelun nopeus usein myös heikkenee tämän myötä. Yrityksen johdon pitäisikin aina punnita tarkkaan palvelinten ulkoistamisen hyödyt ja haitat ennen päätöksen tekoa.

2.2 Vaadittavat resurssit

Riippuen palvelinverkon laajuudesta sekä tallennetun tiedon tärkeydestä, voidaan toimintavarmuuteen panostaa erilaisissa asioissa. Pienelle yritykselle voi riittää yksikin fyysinen palvelin säilytettäväksi omissa tiloissa, mutta palvelin palveluita tarjoava yritys tarvitsee todella varman toimintaympäristön ja useita erilaisia varajärjestelmiä katastrofin varalta. Tässä projektissa tallennustilaa on käyttöjärjestelmälle ja tallennettavalle tiedolle yhteensä vain 80 GB. Sen pitäisi riittää testikäyttöön helposti, koska varsinaista dataa ei tallenneta palvelimelle juuri ollenkaan. Todelliseen käyttöön tarkoitetussa palvelinverkossa voidaan tarvita helposti satakertainen määrä tallennustilaa.

Palvelinverkon tärkein tehtävä on pitää tieto tallessa. Missään tilanteessa ei saisi käydä niin, että jonkun yllättävän ongelman seurauksena tietoa katoaisi peruuttamattomasti. Tämän takia jokaisessa palvelimessa tieto tallennetaan aina kahdelle eri kovalevylle RAID (Redundant Array of Independent Disks) -tekniikan avulla. Tärkein informaatio voi myös olla tallennettuna toisella palvelimella riittävän matkan päässä esimerkiksi tulipalon mahdollisuuden vuoksi. Tiedon hajauttaminen eri paikkoihin riittää poistamaan kovalevyjen hajoamisesta koituvan riskin. Suuri määrä palvelimia tuottaa suuren määrän lämpöä, joten tilan pitäisi olla suuri, kuiva ja hyvin ilmastoitu. Liika kuumuus lyhentää laitteiden käyttöaikaa ja lisää palvelun epävarmuutta sekä laitteiden hankinnasta koituvia kuluja. Uusia palvelinkoneita pitää myös riittää varastossa, koska

laitevikoja ilmenee kuitenkin väistämättä. Tiedon saatavuus on myös oleellinen asia. Esimerkiksi sähkökatkoksen sattuessa pitäisi suurella palvelinverkolla olla oma virtalähteensä.

Palvelinverkot voivat myös joutua verkkohyökkäyksen uhriksi. Erilaiset tietoturvaratkaisut ovatkin oleellisia kun suunnitellaan palvelinverkkoa yritykselle. Mikä tahansa yritys vaatii sekä oikein asennetun palomuurin, että toimivan viruksentorjunta ohjelmiston. Hyökkäyksien tarkoitus voi olla varastaa tietoa palvelimilta tai kuormittaa palvelimia hidastaen niitä merkittävästi. Suuret palvelinverkot houkuttavat hakkereita ja vetävät enemmän hyökkäyksiä. Esimerkiksi useista eri lähteistä palvelimia kuormittava palvelinestohyökkäys, DDoS (Distributed Denial of Service), voi olla hyvin toteutettuna todella hankala estettävä.

3 Tekninen pohjustus

3.1 Virtuaalisointi

Käyttöjärjestelmien virtuaalisointi on 1990-luvulla kehitetty tekniikka, jonka ajatuksena on käyttää yhdellä laitteella samanaikaisesti useita käyttöjärjestelmiä. Pohjalla voi nykyään toimia lähes mikä tahansa käyttöjärjestelmä, kuten esimerkiksi Windows 7. Pohjalla toimivaan käyttöjärjestelmään voidaan asentaa ohjelma, joka luo uuden käyttöjärjestelmän levykuvasta, välittää sille määrätyn osan laitteen resursseista, sekä luo terminaalin virtuaalisen käyttöjärjestelmän käyttämiseen.

Virtuaalisoinnin avulla voi käyttää ohjelmia, joita oma käyttöjärjestelmä ei tue. Esimerkiksi asentamalla Linux-käyttöjärjestelmään virtuaalisointityökalun voi käyttää myös ainoastaan Windowsin tukemia ohjelmia Linuxista luopumatta. Palvelinympäristössä virtuaalisoinnin suurimmat hyödyt tulevat kuitenkin esiin tiedon hallinnassa ja resurssien optimoinnissa. Virtuaalikonetta pystytään helposti optimoimaan sen tarpeiden mukaan lisäämällä tai poistamalla muistia tai prosessointitehoa. Virtuaalinen käyttöjärjestelmä on tallennettu isäntäkoneelle yhteen tiedostoon tai useampaan tiedostoon yhdessä kansiossa, joten sen kopioiminen, siirtäminen tai poistaminen on todella helppoa. Esimerkiksi tehtäessä suuria muutoksia palvelinverkkoon voidaan alkuperäinen kokoonpano kopioida ja palauttaa, mikäli tehdyt muutokset eivät olleet halutunlaisia tai

muutoksia tehtäessä on sattunut virhe. Virtuaalikoneen voi myös pysäyttää milloin vain, jolloin sen viemät resurssit vapautuvat taas hetkeksi uuteen käyttöön. Virtuaalikoneen käyttöä saa halutessa jatkettua tämän jälkeen samasta pisteestä. Virtuaaliohjelmistoja on kahdenlaisia. ”Bare metal” tarkoittaa sitä että virtuaalikoneet toimivat käyttöjärjestelmäytimen päällä, jota ohjataan virtuaalikoneilta. Tällä tavoin isäntäkoneen datajälki on mahdollisimman pieni. ”Non-bare metal” tarkoittaa tavallisen käyttöjärjestelmän yhteydessä toimivaa ohjelmistoa, joka hallitsee virtuaalikoneita. Uusimpia ominaisuuksia virtuaalisointiohjelmissa on niin kutsuttu reaaliaikainen migraatio. Tällä on mahdollista siirtää virtuaalikone fyysiseltä koneelta toiselle, pitäen sen toiminnassa koko siirron ajan. Näin saadaan esimerkiksi huollettua laitteita ilman katkoa palveluissa. Palvelimilla on nykyään myös mahdollisuus tunnistaa ja korjata itsenäisesti ongelmatilanteita. Automatisoitu reaktio tietynlaiseen vikatilaan nopeuttaa huomattavasti palautumista yleisimmistä ongelmista ja parantaa palvelun laatua. Esimerkiksi fyysisessä koneessa oleva vika saa koneella olevan virtuaalikoneen käynnistymään toisella fyysisellä koneella. Vaihtoehtoisesti virtuaalikoneen käyttöjärjestelmässä ilmenevä vika saa sen käynnistymään uudestaan samalla koneella. [1.]

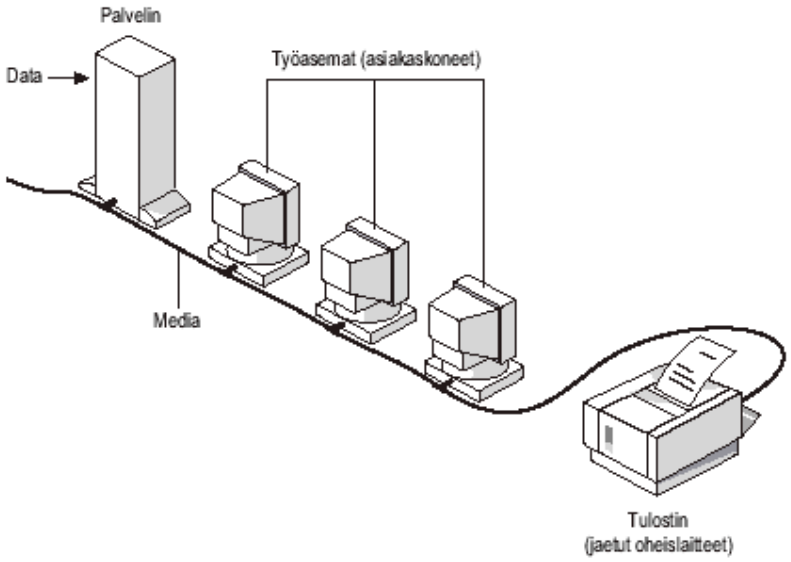
Yksi tapa käyttää käyttöjärjestelmien virtuaalisointia on Virtual Desktop Infrastructure (VDI). Tässä käyttäjän käyttöpääte ottaa yhteyttä palvelimeen, joka luo hänelle oman virtuaalisen työpöytänsä. Kaikki tarvittavat ohjelmat voidaan asentaa palvelimelle, jolta käsin käyttäjät sitten käyttävät niitä. Näin toteutettuna itse käyttöpääte vaatii paljon vähemmän resursseja, kuin jos se itse pitäisi ohjelmia käynnissä. Kun kaikki päätteet eivät kuitenkaan ole koskaan käytössä, voidaan tällä tavalla säästää laite- sekä lisenssikustannuksissa. Lisäksi, jos käyttäjiä on tavallista vähemmän, saavat he koko kapasiteetin käyttöönsä. [2.]

Virtuaalisointia voidaan käyttää käyttöjärjestelmien lisäksi myös ohjelmien virtuaalisointiin, jolloin päästään eroon erilaisista ohjelmistovaatimuksista. Esimerkiksi jotkin ohjelmat tukevat vain Javan vanhempia versioita, eikä useampaa Java versiota missään nimessä kannata pitää yrityksen kaikilla koneilla. Sovelluksen virtuaalisointi paketoi ohjelman vaadittavine ominaisuuksineen, ja tämä voidaan toimittaa suoraan käyttäjän päätteelle. [3.]

3.2 Palvelinverkot

Palvelinverkko on lähiverkko eli Local Area Network (LAN), johon on liitetty vähintään yksi palvelin. Ilman palvelinta toimivaa lähiverkkoa kutsutaan vertaisverkoksi. Lähiverkko taas on rajatulla alueella toimiva tietoliikenneverkko. Lähiverkon laitteet on kytketty toisiinsa tavallisesti kytkimillä, ja lähiverkko on yhteydessä laajaverkkoon, eli Wide Area Networkiin (WAN), reitittimen avulla. Palvelinverkko määritellään toimialueeseen, joka määrittää, mitkä laitteet kuuluvat palvelinverkon piiriin.

Palvelinverkon suurimmat hyödyt verrattuna vertaisverkkoon ovat verkon helpompi hallinnointi, parempi tietosuoja sekä yhteinen tietovarasto. Palvelimen kautta pystytään asentamaan kaikille keskitetysti samat ohjelmistot. Tällöin voidaan olla varmoja, että käyttöpäätteistä löytyy tarvittavat ohjelmistot ja päivitykset. Myös käyttäjätilien ja niihin liitettyjen oikeuksien muokkaaminen tapahtuu palvelimen kautta. Myös palomuurien hallinnointi onnistuu helpommin yhdellä palvelimella kuin usealla eri tietokoneella. Palvelimelle saa jaettua tiedostojen lisäksi myös ohjelmia verkon jäsenten käyttöön. Kuvassa 1 on kuvattuna yksinkertainen palvelinverkko [Kuva 1.] [4;5.]



Kuva 1. Yksinkertainen palvelinverkko. [6.]

4 Palvelinympäristön suunnittelu

4.1 Fyysiset laitteet

Vaikka palvelinkoneet käyttävätkin samoja käyttöjärjestelmiä ja tekniikoita kuin muut tietokoneet, on niissä käyttötarpeen mukaan panostettu lähinnä tiedon siirtoon ja tallennukseen vaikuttaviin asioihin. Muisti, tallennustila ja prosessointi ovat tärkeimpiä ominaisuuksia. Esimerkiksi näyttöä kelpaa ohjaamaan mikä tahansa tarkoitukseen valmistettu ohjain, eikä emolevy tarvitse mitään erityisiä liitäntöjä. Taulukossa 1 on nähtävissä modernin palvelinkoneen ominaisuuksia. Dell PowerEdge VRTX tukee jopa 768 GB muistia sekä 48 TB tallennustilaa. Siinä on lisäksi lukuisia ulkoisia ja sisäisiä verkkoportteja, tehokas jäähdytinjärjestelmä, sekä muita erityisiä ominaisuuksia. [7.]

Palvelimet vievät paljon tilaa ja synnyttävät paljon melua sekä lämpöä. Tämän takia niille kannattaa varata oma tilansa. Hyvin sopii esimerkiksi kellarikerroksen ympäri vuoden viileä lämpötila yhdistettynä hyvään ilmastointiin. Sähköä varaava ja virtapiikkejä tasoittava UPS (Uninterruptible Power Supply) olisi myös hyvä järjestää varsinkin sähkökatkosten varalle. Tässä kohtaa tulisi jo tietää, paljonko laitteita ja käyttäjiä palvelinverkkoon tultaisiin liittämään ja mitä eri resursseja palvelinten tulisi tarjota. Nämä seikat vaikuttavat palvelinten määriin sekä palvelinten laitteistovaatimuksiin. Verkkoa pystyy toki myöhemmin laajentamaan, mutta siihen liittyy usein paljon enemmän työtä. Kannattaa siis suunnitella palvelinverkko huolella ennen hankintojen tekemistä.

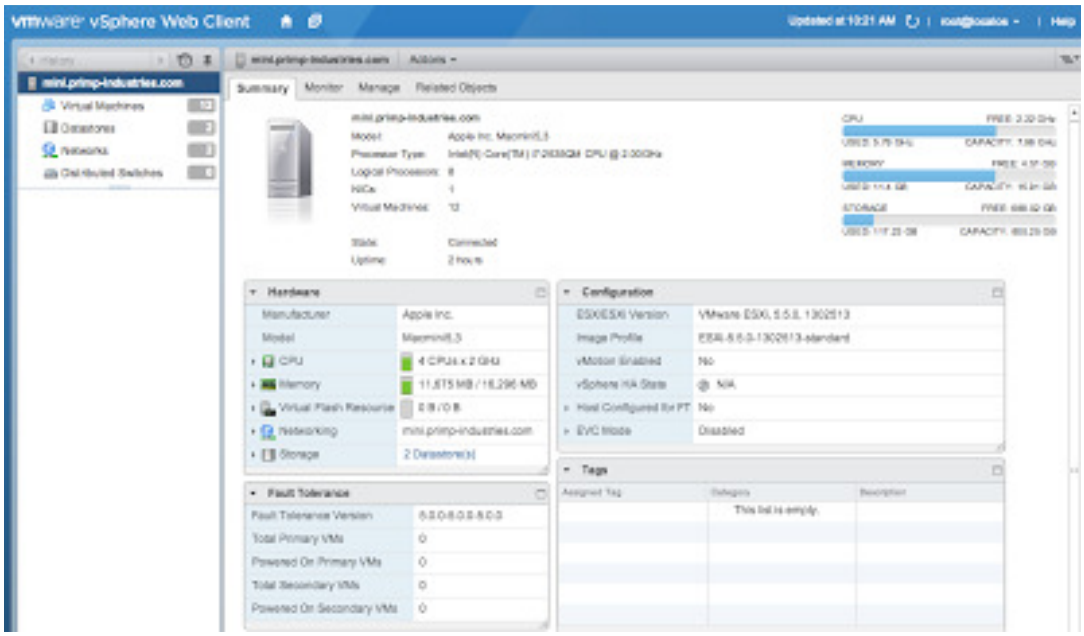
Palvelinverkon roolit jaetaan yhdelle tai useammalle palvelimelle. Tiettyjen roolien takia monipuolisen ja toimintavarman palvelinverkon rakennukseen tarvitaan usein useampia palvelimia. Toimintavarmuuden takaamiseksi tulisi verkossa olla vähintään kaksi toimialueen ohjainta eli Domain Controlleria (DC). Lisäksi ainakaan Windows-palvelinverkon DC:lle ei tulisi asentaa Structured Query Language (SQL) -palvelinta tai sähköpostipalvelinta, sillä nämä saattavat sekoittaa tai hidastaa toistensa toimintaa. Lisäksi kannattaa ajatella roolien jakamista yleistä toimintavarmuutta silmällä pitäen. Esimerkiksi jos käytetään pikaviestintä ja sähköpostia, olisi järkevää jakaa ne eri palvelimille. Mikäli toinen palvelimista sattuisi kaatumaan, olisi toinen viestintämekanismi vielä toiminnassa. [8.]

4.2 Käyttöjärjestelmien valinta

Isäntäkoneen käyttöjärjestelmän tulisi olla erittäin toimintavarma. Sen kaatuminen virtuaalisessa palvelinympäristössä johtaisi muidenkin palvelimien kaatumiseen, kun taas virtuaalisen vieraskoneen kaatuminen ei vaikuta muiden virtuaalikoneiden käyttöjärjestelmien toimintaan. Isäntäkoneeksi kannattaa myös valita käyttöjärjestelmä, jonka käyttö vaatii eniten grafiikkaa ja muokkausta. Windows on tietoturvan kannalta hieman muita huonompi käyttöjärjestelmä isäntäkoneelle, sillä suurin osa haittaohjelmista suunnitellaan juuri sitä vastaan. Virtuaalisointiin on kehitetty erikseen muutamia käyttöjärjestelmiä, jotka sisältävät itsessään jo työkalut virtuaalisen palvelinverkon ylläpitoon. Muut käyttöjärjestelmät vaativat erikseen ohjelmiston asennuksen tehtävää varten. Eri ratkaisut sopivat eri tilanteisiin riippuen palvelinten tehtävistä.

Microsoft valmistaa yrityskäyttöön helposti kokonaisuuksiksi muotoiltavia paketteja. Ne eivät ole kevyimmästä päästä, mutta ne ovat helppokäyttöisiä ja niihin saa hyvin tukea. Erityisesti palvelinkäyttöön tarkoitetut Windows Server 2008 sekä Windows Server 2012 ovat hyviä ratkaisuja yrityksen tarpeisiin. Windows-palvelimet eivät kuitenkaan ole aivan yhtä toimintavarmoja kuin yksinkertaisemmat, virtuaalisointiin tarkoitetut käyttöjärjestelmät. Tämän takia voi olla järkevää asentaa virtuaaliset Windows-palvelimet jollekin muulle alustalle. Windows tarjoaa kuitenkin käyttöjärjestelmän ohella myös oman virtuaalisointityökalunsa, Hyper-Vn, johon kannattaa tutustua. Hyper-V löytyy edellä mainittujen käyttöjärjestelmien lisäksi myös Windows 8:sta.

EXSi on WMwaren kehittämä käyttöjärjestelmä virtuaalisointiin. Se tarjoaa ainoastaan käyttöjärjestelmäytimen sekä kevyen käyttöliittymän, vSphere Clientin [Kuva 2.], jonka se asentaa virtuaalikoneelle. Se vaatii ainoastaan 150 MB levytilaa ollen kevyt ja yksinkertainen. Se on siten myös toimintavarma ja tietoturvallinen, ja se on tarkoitettu juuri isäntäkoneen käyttöjärjestelmäksi. ESXi on hyvä vaihtoehto, varsinkin jos muut käytetyt käyttöjärjestelmät ovat liian epävakaita isäntäkoneen rooliin, tai jos verkon kaikki palvelimet tulee asentaa virtuaalisesti jostain muusta syystä. [9.]



Kuva 2. ESXi 5.0 käyttöjärjestelmää hallitaan virtuaalikoneelle asennettavan vSphere Clientin kautta. [10.]

Monien muiden muassa Red Hat käyttää avoimen lähdekoodin tekniikkaa palvelimissaan. Linux on eri tutkimusten mukaan tehokkuudessa ja hinnoittelussa Windowsia parempi ratkaisu. Palvelimissa Linux onkin jo huomattavasti yleisempi kuin Windows. Windows on kuitenkin joskus yhteensopivuutensa takia ainoa järkevä ratkaisu. Avoimien lähdekoodin käyttöjärjestelmien yhteisenä ongelmana on taas aina standardoinnin puute. Lähes kaikki ohjelmistot tukevat Windowsia, mutta Linuxille tämän toteuttaminen on selvästi haastavampi tehtävä. Tämä johtuu siitä, että kehittäjiä on useampia, eikä yksi taho valvo kehitystä. Tämän takia Red Hat tarjoaakin enemmän kokonaisia ratkaisuja yksittäisten ohjelmistojen sijaan. Käyttöpäätteille Linuxiin pohjautuvat käyttöjärjestelmät eivät ole vielä tulleet käyttöön samassa mittakaavassa kuin palvelimiin. Ihmiset ovat ehkä liiankin tottuneet käyttämään Windows-käyttöjärjestelmiä, joten Windows tulee todennäköisesti säilyttämään asemansa. [11.]

Citrix on johtavia yrityksiä virtuaalisoinnin alalla, ja myös sillä on oma virtuaalisointiin tarkoitettu käyttöjärjestelmänsä. XenServer on myös avoimen lähdekoodin käyttöjärjestelmä, ja se on ilmainen kaikille. Siihen voi kuitenkin ostaa lisenssin, jonka mukana tulee käyttötuki. Se on kevyt ja tarjoaa osaavalle käyttäjälle kaikki tarvittavat työkalut suurenkin palvelinympäristön ylläpitoon. Siitä puuttuu muutamia

ominaisuuksia, mutta ilmainen ohjelma houkuttaa. Osa käyttäjistä on todennut XenServerin vaikeakäyttöiseksi, mutta siitä huolimatta se on erittäin suosittu. Mikäli budjetti on pieni ja pienet puutteet ominaisuuksissa eivät haittaa, on XenServer hyvä ratkaisu palvelinverkon ylläpitoon. [12]

4.3 Virtuaalisointiohjelmistot

Taulukko 1. Virtuaaliohjelmien vertailu on vaikeaa, kun eri ohjelmat toteuttavat samat asiat hieman eri tavalla. Taulukossa on näkyvissä muutamia suorituskyvyn kannalta tärkeitä ominaisuuksia.

	Wmware vSphere 5.5	Wmware Workstaton 10	Microsoft Hyper-V 2012	Oracle Virtualbox 4.3	Red Hat KVM	Citrix XenServer 6.2
”Bare metal”	x		x		x	x
Dynamic memory control	x	x	x	x	x	x
Live migration	x	x	x	x	x	x
Full screen		x				
Freeware				x		x
Open Source					x	x
Max RAM / Host	4TB	?	4TB	No limit		1TB
Max RAM / VM	1TB	64GB	1TB	No limit	512GB	128GB
Max size for VM hard disk	62TB	8TB	64TB	2TB	Depends on filesystem	2TB
Max CPUs per VM	64	16	64	32	32	16
USB support	USB 3.0	USB 3.0	USB 3.0	USB 2.0	USB 3.0	USB 3.0 (partially)

WMware on aina ollut käyttöjärjestelmien virtuaalisoinnin edelläkävijä. Se oli ensimmäinen yritys, joka toi yleisimpiin käyttöjärjestelmiin yhteensopivan virtuaalisointialustan markkinoille. Lähes jokainen suuri palvelin palveluita tarjoava yritys käyttää WMwarea. WMware tarjoaa ainoana sekä kilpailukykyisen ”bare metal” sekä ”non-bare metal” virtualisointiohjelmiston. Se on vielä toistaiseksi lähes kaikilla osa-alueilla kilpailijoitaan edellä, mikä näkyy hyvin vastaavia eri ohjelmia vertailevassa taulukossa [Taulukko 1]. Se saattaa olla kallis, mutta on täysin hintansa arvoinen, mikäli sen lukuisia ominaisuuksia pystyy hyödyntämään.

Red Hat kehittää Linuxiin pohjautuvien palvelimien lisäksi myös virtuaalisointia. Red Hatin tuotteet ovat kilpailijoihin nähden edullisia myös virtuaalisoinnin osalta, mutta teknisellä puolella ei ole aivan terävintä kärkeä. Red Hat tarjoaa kuitenkin toimivia ratkaisuita suuremmillekin yrityksille, jotka haluavat siirtyä virtuaaliseen toimintaympäristöön. Red Hatin hyvä puoli tässä kohtaa verrattuna esimerkiksi

WMwareen on kokonaisvaltaisemmat ja edullisemmat ratkaisut.

Virtualbox on Oraclen avoimen lähdekoodin virtuaalisointiohjelma. Siitä löytyy kaupallisen version lisäksi hieman ominaisuuksiltaan vähäisempi ilmainen versio yksityisiä käyttäjiä varten. Kaupallinen versio ei ominaisuuksiltaan pärjää vertailussa, mutta yksityiskäyttöön sopiva ilmaisversio on kevyt käyttää ja erittäin suosittu.

Citrix tarjoaa XenServerin muodossa myös virtuaalisointiin tarvittavat työkalut. Tämän lisäksi Citrix toimittaa pilvipalveluita, verkkoratkaisuja sekä muuttaa ohjelmistoja ja työpöytiä virtuaaliseksi. Se on aikaisemmin toiminut paljon yhteistyössä Microsoftin kanssa. Tästä voisi päätellä, että Citrix ei todennäköisesti tulekaan keskittymään käyttöjärjestelmien virtuaalisointiin, vaan jatkaa muiden palveluiden virtuaalisoinnin parissa. Citrix on myös paljon käytetty tuotemerkki yritysmaailmassa.

Hyper-v on Microsoftin oma ratkaisu virtuaalisointiin, ja se on tutkimuksien mukaan paras ratkaisu Windows-käyttöjärjestelmiä virtualisoitaessa. Se löytyy vakiona Windows Server 2012:sta sekä Windows 8:sta. Se tukee myös yleisimpiä Linux-käyttöjärjestelmiä virtuaalikoneina, mutta isäntäkoneen käyttöjärjestelmäksi sille kelpaa ainoastaan Windows-käyttöjärjestelmä.

4.4 Palvelinten roolit

Palvelimilla ajatellaan olevan tietyt roolit, jotta päästäisiin helpommin hahmottamaan palvelinverkon eri osat helpommin. Yksi rooli kuvaa yhtä tehtävää, ja tehtäviä voi olla useampia yhdellä palvelimella. Jotkin roolit tulee asentaa erikseen toisistaan, ja jotkin roolit vaativat toista roolia toimiakseen. Esimerkiksi Windows-ympäristössä sähköpostipalvelin tarvitsee käyttöönsä Web-palvelimen, mutta sitä ei voi kuitenkaan asentaa samalle käyttöjärjestelmälle hakemistopalvelun kanssa. Palvelimella voi olla useita rooleja, joihin liittyy useita erilaisia ominaisuuksia. Tässä luetellaan muutamia yleisimpiä rooleja, jotka asennetaan myös tässä projektissa.

4.4.1 Domain Controller (DC)

DC vastaa Windows-palvelinympäristön toimialueen tunnistekyselyihin, kuten toimialueen kirjautumiseen. Se säilyttää käyttäjätietoja sekä pakottaa tietoturvasäännöt toimialueen käyttäjille. DC:lla ei ole paljon tehtäviä, mutta ainakin yksi DC on välttämätön toimialueen toimivuuden kannalta. Näitä kannattaa aina luoda useampi siltä varalta, että se ainoa kaatuu. DC saattaa aiheuttaa ongelmia asennettuna samalle käyttöjärjestelmälle tiettyjen roolien kanssa. Ongelman voi kiertää esimerkiksi asentamalla roolit DC-roolin omaavalla koneella olevalle virtuaaliselle palvelimelle. [13.]

4.4.2 Domain Name Server (DNS)

Toimialueen ensimmäistä DC:a määrittäessä kannattaa palvelin määritellä myös verkon DNS-palvelimeksi. DNS-palvelin on nimipalvelin, joka muuttaa sille annetut nimet Internet Protocol (IP) -osoitteiksi. Toimialueen verkkoon liitetyt koneen voivat lähettää tälle nimen tai verkko-osoitteen, ja DNS yrittää selvittää sille kuuluvan IP-osoitteen. Mikäli osoitetta ei löydy toimialueen verkosta, kysely lähetetään eteenpäin Internet Service Providerille (ISP). Verkkotunnukset koostuvat eri tunnuksen tasoista, jotka erotetaan toisistaan pisteillä. Esimerkiksi:

Virtualserver.AD1.Imgcorp

Tässä VirtualServer on alin tunnus, ja osoittaa palvelimeen. AD1 on hakemiston nimi ja Imgcorp toimialueen nimi. Tunnuksen taso kasvaa aina vasemmalta oikealle. DNS käy tunnuksen läpi vasemmalta oikealle ja ohjaa ensimmäisen tunnistamansa tunnuksen IP-osoitteen mukaan. [14.]

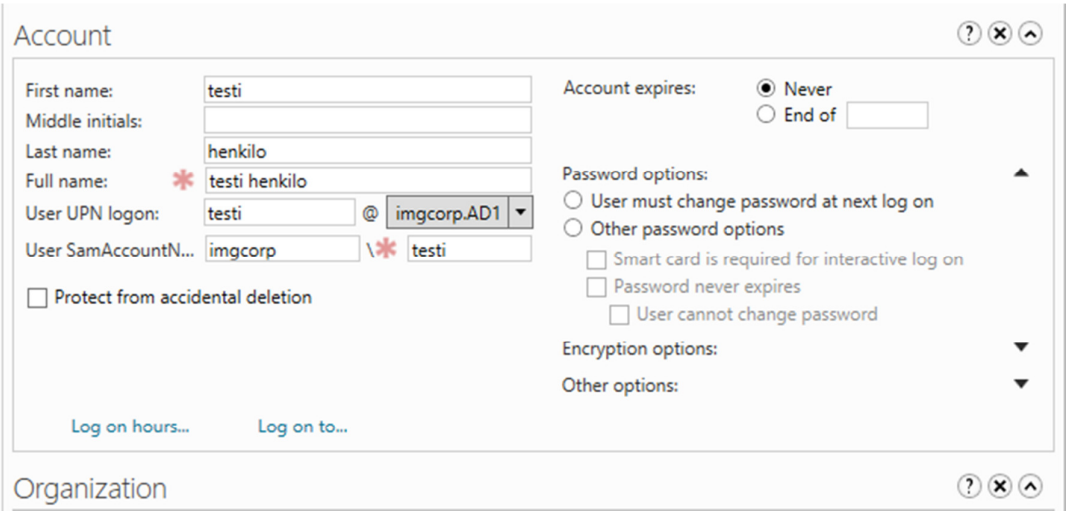
4.4.3 Dynamic Host Configuration Protocol (DHCP)

DHCP välittää toimialueen verkkoon liitettäville laitteille verkkoasetuksia. Se välittää esimerkiksi kannettavalle tietokoneelle IP-osoitteen, kun se liitetään verkkoon. Kun kyseinen tietokone lähtee verkosta, sen osoite vapautuu DHCP:lle uudelleen käytettäväksi. DHCP:lle määritetään tietty alue, jolta se voi jakaa osoitteita. DHCP automatisoi verkkoasetuksien käsin muokkaamista huomattavasti. Sillä voidaan myös säästää paljon osoitetilaa, jos suuri osa toimialueen koneista ei ole samanaikaisesti verkossa. [15.]

4.4.4 Toimialueen hakemistopalvelu

Active Directory Domain Services (ADDS), jonka vanhempi ja useammin käytetty nimitys on Active Directory (AD), on Windows-verkkojen jaettu hakemistopalvelu. Sille on myös Linux-pohjaisia vaihtoehtoja, mutta niiden lisääminen Windows-ympäristöön lopettaa Microsoftin käyttötuen kokonaan palvelinverkon osalta. Mikäli kuitenkin haluaa päästä eroon Microsoftin tuotteista, voi saman toiminnallisuuden saada vaikka avoimen lähdekoodin OpenLDAP-ohjelmistoon pohjautuvilla ohjelmilla. ADDS:n kautta voi hallinnoida yhtä tai useampaakin toimialuetta. ADDS yhdistää kaikki palvelinverkon eri roolit, laitteet ja käyttäjät. Sillä on tyypillisesti kolme eri käyttötarkoitusta. Se toimii sisäisenä hakemistona yrityksen omille työntekijöille, johon ulkopuoliset eivät pääse käsiksi. Se voi toimia ulkoisena hakemistona asiakkaille ja yhteistyökumppaneille, joka sijaitsee yrityksen verkon ja internetin välissä. Se voi myös olla ohjelmistohakemisto jollekin sitä käyttävälle ohjelmalle, joka saa esimerkiksi SQL-kyselyillä haettua tietoa omiin tarkoituksiinsa.

ADDS käyttää kaiken perustana objekteja, joita ovat konetilit, käyttäjät ja ryhmät. Jokainen käyttäjätili, esimerkkinä kuvassa 3 näkyvä tili, luodaan Active Directory Administrative Centerissa (ADAC) ennen kuin käyttäjä voi kirjautua toimialueeseen. Kun käyttäjä kirjautuu koneellaan toimialueeseen, ADDS luo koneelle oman konetilin. Näillä tileillä ADDS tunnistaa eri laitteet ja käyttäjät ja pystyy hallitsemaan niitä. Kaikkia kenttiä, nimiä ja salasanoja pystyy vapaasti muokkaamaan ADAC:n kautta.

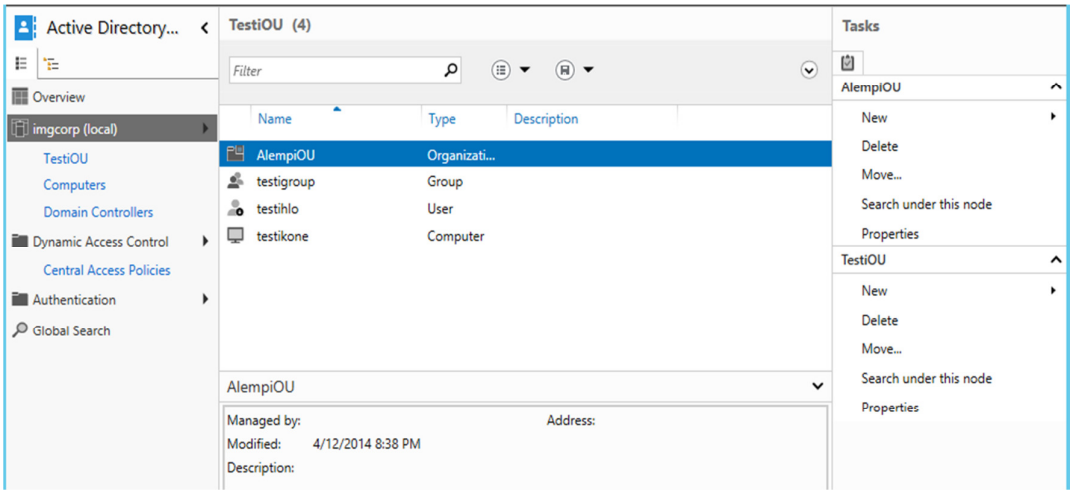


Kuva 3. Käyttäjätunnuksen tietoja Windows Server 2012: n Active Directoryssa. Nähtävien ominaisuuksien lisäksi tunnukseen on liitetty muun muassa organisaatiosta, käyttäjän ryhmistä, salasana asetuksista, paikallisesta käyttäjäprofiilista sekä käyttäjään liitetyistä ryhmäkäytännöistä.

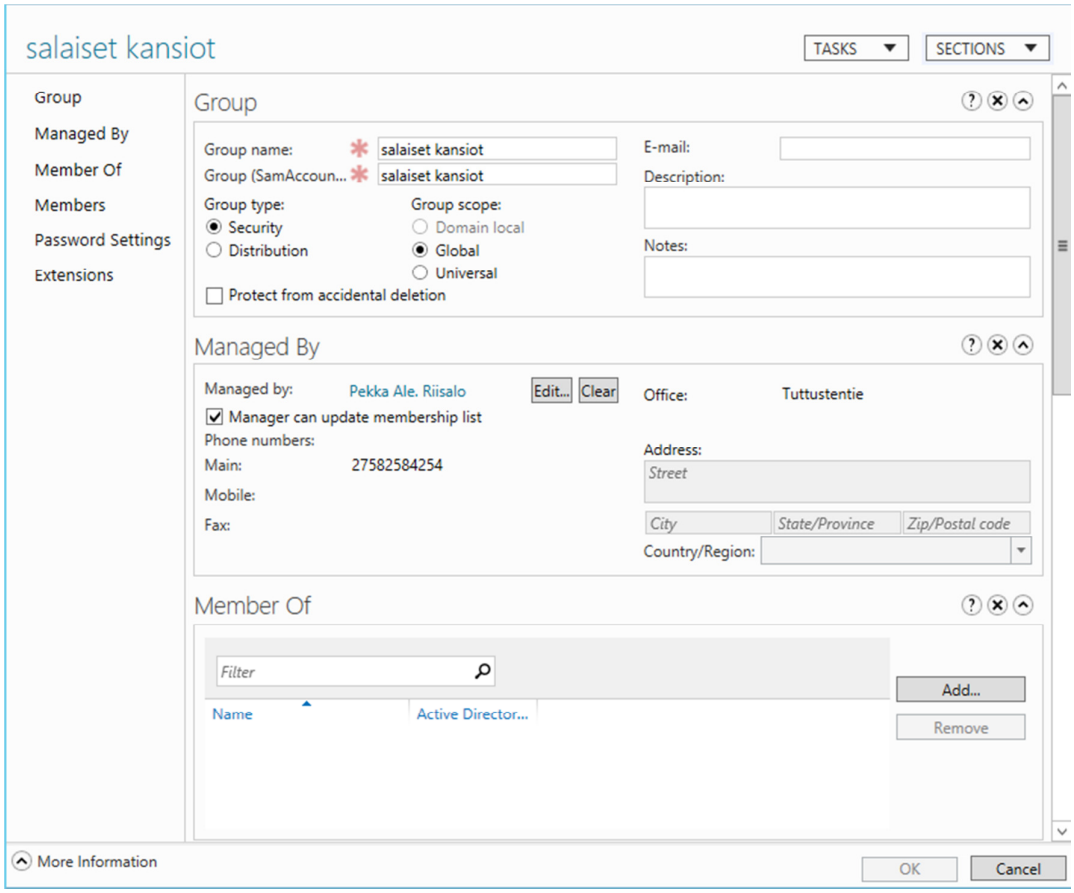
Kaikki käyttäjät ja koneet kuuluvat aina johonkin organisaatioyksikköön, jonka mukaan ne luokitellaan. Yrityksessä luokittelun kriteeriksi valitaan tyypillisesti objektin fyysinen sijainti. Helsingissä työskentelevän käyttäjän organisaatioyksikkö voisi olla esimerkiksi:

Imgcorp.local\EU\Suomi\Helsinki\Käyttäjät

Tässä Imgcorp.local on yrityksen toimialue. Toimialueiden toimintaa havainnollistaa kuva 5. Organisaatioyksikön lisäksi käyttäjiä voidaan luokitella erilaisiin ryhmiin, joille voidaan antaa erilaisia oikeuksia. Ryhmillä voi olla oikeuksia verkkolevyillä sijaitseviin kansioihin, sähköpostilaatikoihin, ohjelmistoihin tai mihin vain, mikä on liitetty palvelinverkkoon. Ryhmiä voi myös käsitellä hyvin vapaasti ja niihin voi helposti lisätä muita ryhmiä ja käyttäjiä. Kuvassa 5 on esimerkkinä ryhmä salaiset kansiot, jolla on oikeudet käyttää kansiota nimeltä Salaiset Kansiot. ADDS sisältää myös oman globaalin hakukoneensa, jonka avulla suurestakin hakemistosta löytää helposti etsimänsä. [16]



Kuva 4. organisaatioyksikköä käsitellään kuten kansiopuuta. Siihen kuuluu ryhmiä, käyttäjiä sekä alihakemistoja, eli alempia organisaatioyksikköjä. Tässä esimerkkinä TestiOU, jonka piiriin kuuluu myös AlempiOU. Organisaatioyksikön rakennetta voi vapaasti muokata



Kuva 5. Ryhmillä on aina omistaja ja näkyvyysalue. Security-tyyppisille ryhmille voi antaa käyttöoikeuksia dataan tai ohjelmistoihin. Distribution-tyyppisiä ryhmiä voi käyttää ainoastaan sähköpostin jakelulistojen luomiseen.

ADDS pystyy myös luomaan luottosuhteita muihin toimialueisiin. Mikäli yrityksellä on muutamia suuria, omina kokonaisuuksinaan toimivia yksittäisiä toimipisteitä, kannattaa niille tehdä omat toimialueensa. Myös toisen yrityksen toimialueen kanssa voi luoda luottosuhteen, jos esimerkiksi ulkoistetaan palveluita. Luottosuhteen laatu voi olla esimerkiksi yksi- tai kaksisuuntainen, ja luottosuhdetta voi määritellä monilla muilla erilaisilla asetuksilla.

Kaikkien asetusten syöttämistä yrityksen koneisiin ei myöskään tarvitse tehdä käsin, sillä ADDS sisältää myös moduulin Windows PowerShell-työkaluun. PowerShell on Windowsin uuden sukupolven komentotyökalu, jonka avulla voi ajaa ”skriptejä”. PowerShellia käyttämällä pystyy automatisoimaan esimerkiksi käyttäjien tai sähköpostilaatikon luomista. Tämä helpottaa varsinkin suurempien käyttäjä- ja konetilien hallintaa. PowerShell on erittäin tehokas työkalu ryhmäkäytäntöjen luomiseen ja ajamiseen. Ku-

vissa 6 ja 7 on esimerkkejä skripteistä, jotka voivat olla hyödyllisiä ryhmäkäytäntöjä määritellessä. [17.]

```
$credential = New-Object System.Management.Automation.PsCredential("coex\administrator", (ConvertTo-
SecureString "P@ssw0rd <mailto:P@ssw0rd>" -AsPlainText -Force))
Add-Computer -DomainName "coex.com" -Credential $credential -passthru
restart-computer
```

Kuva 6. Tämä skripti liittää koneen toimialueeseen DomainName. [18.]

```
$dom = [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()
$root = $dom.GetDirectoryEntry()
$search = [System.DirectoryServices.DirectorySearcher]$root
$search.filter = "(&(objectclass=computer)(name=windowsserver))"
$search.findall() | %{$_.GetDirectoryEntry() } | %{$_.DeleteObject(0)}
```

Kuva 7. Tämä skripti käynnistää tietokoneen uudelleen. [18.]

Group Policy Management Console (GPMC) on työkalu, jonka kautta voidaan hallinnoida tiettyihin ryhmiin kuuluvien käyttäjien asetuksia, eli ryhmäkäytäntöjä. Sillä pystytään automaattisesti muuttamaan käyttäjän asetukset halutun laisiksi. Voidaan esimerkiksi päättää, menevätkö toimialueen koneet automaattisesti virransäästötilaan halutun ajan kuluessa. Voidaan myös luoda erillinen ryhmä, joihin kuuluviin koneisiin tämä sääntö ei koske. ryhmäkäytännöt päivittyvät automaattisesti koneen ollessa toimialueen verkossa. [19.]

4.4.5 Sähköpostipalvelin

Oma sähköpostipalvelin on ehdoton työkalu yritykselle. Se auttaa pitämään yrityksen viestit sen omana tietona, mahdollistaa sähköpostiliikenteen ohjaamisen sekä arkistoi sähköpostit talteen, jotta niitä voidaan tarvittaessa tarkastella jälkeenpäin. Kaupallisista tuotteista MS Exchange on selvästi paras valinta Windows-verkkoihin. Avoimen lähdekoodin sähköpostipalvelimia on useita. Esimerkiksi hMailServer on hyvä valinta, mikäli ei tarvita toimivan sähköpostin lisäksi muita ominaisuuksia. Muista sähköpostipalvelimista ei esimerkiksi löydy Exchangessa paljon käytettyä kalenteria. Exchangen ja Outlookin yhdistelmä antaa muitakin ominaisuuksia, joita muut Windows-käyttöjärjestelmälle suunnitellut sähköpostipalvelimet eivät tarjoa. Windows-verkoissa

on kuitenkin mahdollista käyttää virtualisoinnin ansiosta vaikka Linux-pohjaista sähköpostipalvelinta. Tällä tavalla saataisiin lähes samat ominaisuudet pienemmällä hinnalla tai jopa ilmaiseksi. Exchange on joka tapauksessa niin paljon käytetty ohjelmisto Windows-verkoissa, että siihen kannattaa perehtyä.

Windows-palvelimia käyttäessä Exchange on kaikin puolin helppo ratkaisu. Microsoft Exchange toimii saumattomasti yhteistyössä ADDS:n kanssa käyttäen samoja käyttäjätietoja sekä ryhmiä. Exchange on kuitenkin suositeltavaa asentaa omalle erilliselle palvelimelle. ADDS ja Exchange saattavat samalla käyttöjärjestelmällä sekoittaa palvelimen toiminnan täydellisesti. Samasta syystä sitä ei myöskään kannata asentaa samalle palvelimelle DC:n kanssa. Työkalut Exchangen hallinnointiin voidaan kuitenkin asentaa ADDS:n kanssa samalle palvelimelle. Tällä tavalla koko palvelinverkon hallinnointiin riittää edelleenkin yhteys yhteen palvelimeen. Virtuaalisoinnista on paljon apua, jos ei haluta asentaa Exchangea varten uutta fyysistä palvelinta. Exchange vaatii kuitenkin huomattavan määrän muistia toimiakseen, mikä pitää ottaa huomioon, kun jakaa rooleja palvelimille. Kun kaikki muut projektissa asennetut roolit toimivat helposti jaetulla 2 GB:n muistilla, Exchange 2013:n toiminta vaatii huikeat 8 GB muistia käyttöönsä. Lisäksi Exchange 2013 ja Windows Server 2012 R2 ovat yhteensopiva ainoastaan toistensa kanssa, joten kevyempää Microsoftin sähköpostipalvelinta ei ole mahdollista asentaa. Exchange 2013:n asennus on helppoa verrattuna edellisiin versioihin. Asennustyökalu asentaa tarvittavat ominaisuudet palvelimelle, ja jos jotain ongelmia asennuksen yhteydessä huomataan, se ilmoittaa ongelman sekä ratkaisun selkokielellä. Asennustyökalun automaattinen virheiden tunnistaminen ja avustaminen on mainostettu ominaisuus jo monissa muissakin ohjelmissa, mutta tässä tapauksessa se vaikuttaa löytävän oikeita ongelmia ja antavan oikeita ratkaisuja. Aikaisemmin sama virheilmoitus on voinut johtua kymmenestä eri asiasta. Ohjelmaa asennettaessa kaikki tarvittavat ominaisuudet lisätään automaattisesti käyttöjärjestelmästä. Mikäli jotain ylimääräistä tarvitaan, asennustyökalu antaa linkin Microsoftin sivuille, mistä puuttuvan ohjelmiston saa ladattua ilmaiseksi. [20.]

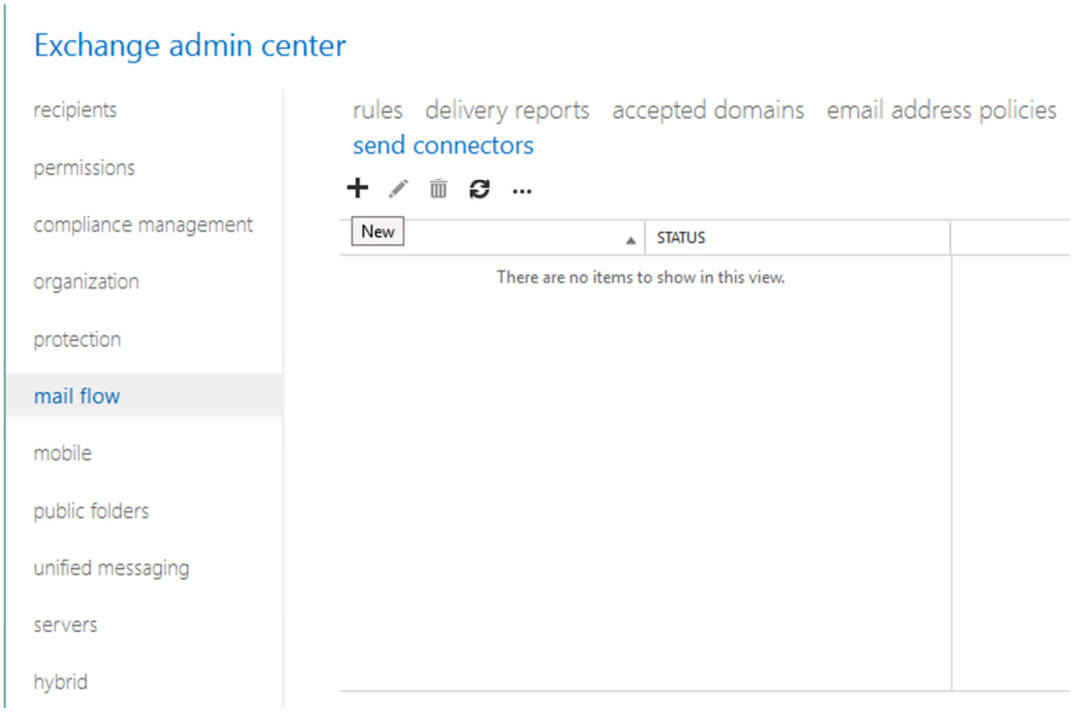
Exchangen toiminta vaatii sekä Mailbox- että Client Access-asennukset ainakin yhdelle palvelimelle. Mailbox pitää sisällään sähköpostilaatikoita sekä julkisten kansioiden tietokantoja. Se myös vastaanottaa käyttäjätilien tiedot, osoitelistat sekä sähköpostiosoitteisiin liitetyt säännöt Active Directorysta. Client Access hyväksyy yhteyden otot käyttäjiltä. Se tukee IMAP4-, POP3-, ActiveSync- ja Outlook Web Access-protokollia. Ex-

change tarvitsee myös ISS:n asennuksen, jota se käyttää Web-pohjaisen käyttöliittymän luomiseen. [20.]

Ohjelmiston asennuksen jälkeen muokataan käyttäjien oikeuksia sekä sähköpostin ohjaus ottamalla selaimen kautta yhteys Client Access-asennuksen omaavaan palvelimeen seuraavalla tavalla:

> Otetaan yhteys palvelimeen selaimen kautta: https://Virtualserver2/ECP
> Mail Flow > Send Connectors > New+ > Syötetään nimi > Internet >
> Valitaan: “MX record is associated with recipient domain”
> Kohdassa “Address space”: Add+
> Kohdassa “Add domain”, valitaan tyypiksi “SMTP” ja syötetään sitten toimialueen täydellinen nimi.
> Varmistetaan ettei ”Scoped send connector” ole valittuna
> Kohdassa ”Source server” valitaan: Add+ > Valitaan palvelin jossa on Mailbox-asennus

Exchangessa voidaan luoda sähköpostilaatikko käyttäjälle, jonka voi yhdistää ADDS:ssa olevaan käyttäjänimeen. Tiliin liitetään näin käyttäjän henkilötietoja ja sen kautta voidaan ohjata ja rajoittaa käyttäjän sähköpostiliikennettä. Tiliin voidaan myös liittää useampia sähköpostiosoitteita. Kuvassa 8 näkyy Exchange 2013:n hallintatyökalu. [21.]



Kuva 8. Exchange Admin Center on työkalu, jolla saadaan ohjattua sähköpostipalvelimen toimintaa. Näkymässä on Exchange 2013.

4.4.6 Internet Information Services

IIS eli Web Server-rooli on useimmiten tarkoitettu Web-sivujen säilytykseen, prosessointiin ja lähetykseen. Sitä voidaan kuitenkin käyttää myös paikallisessa verkossa esimerkiksi tulostimien tai reitittimien yhteydessä lähettämään dataa laitteen toiminnasta, tai muodostamaan käyttäjälle rajapinnan laitteeseen. Web Server tarvitaan myös muun muassa VPN:n ja Exchangen käyttöön. Tämän kautta Exchange tarjoaa web-pohjaisen käyttöliittymän sähköpostipalveluun ja VPN oman kirjautumispalvelunsa Internetin välityksellä. Myös monet muut roolit käyttävät IIS:n toimintoja hyväkseen. [22.]

4.4.7 Järjestelmänhallintaohjelmistot

Järjestelmänhallintaohjelmistot on tarkoitettu hallitsemaan suuria määriä tietokoneita. Ne tarjoavat ratkaisuja etäkäytön hallintaan, päivitysten ja ohjelmistojen asennukseen sekä verkon tietoturvaan. Järjestelmänhallinta työkalut ovat myös hyvä keino valvoa verkon tietokoneita. Tällainen ohjelmisto ei ole pakollinen hankinta yrityksille, joiden käyttöpäätteiden lukumäärä on muutamia kymmeniä. Suurempi määrä koneita vaatisi

jo liian suuren työmäärän, jos pitäisi esimerkiksi tarkistaa jokaisesta jokin tietty ominaisuus. Järjestelmänhallintaohjelmiston avulla työasemien ominaisuuksia voi tutkia suurina määrinä kerrallaan. Se suorittaa SQL-kyselyitä, joiden mukaan se luokittelee työasemia valitun ominaisuuden mukaan. Tämän takia se vaatii SQL-palvelimen toimiakseen. Riippuu paljon verkon laajuudesta ja muista järjestelmistä, mitä tuotetta kannattaa käyttää. Kaikki vastaavat järjestelmät ovat myös ominaisuuksiltaan vain hieman erilaiset. On vaikea määritellä, mikä seuraavista on yleisesti paras vaihtoehto, sillä niiden eri ominaisuudet vastaavat hyvin eri tarpeisiin.

Mikäli verkko on todella suuri ja laitteisto koostuu puhtaasti Microsoftin tuotteista, MS System Center on hyvä valinta. Se istuu Windows-ympäristöön ja toimii samalla logiikalla kuin muutkin Microsoftin tuotteet. Microsoftin yleisyys myös puoltaa System Centerin valintaa, sillä sen osaajia löytyy helposti. System Center on kuitenkin kallis hankinta pienelle yritykselle. Sen ominaisuuksista ei myöskään saa kaikkea irti, ellei verkossa ole todella paljon hallittavia koneita. Eri yritykset tarjoavat edullisempiakin ratkaisuja pienemmän mittakaavan palvelinverkkoihin.

Symantecin Altiris on parempi järjestelmä keskisuurelle yritykselle sen edullisuuden takia. Microsoftin System Center maksaa yksittäisenä ohjelmistona saman määrän, riippumatta siitä, mitä ominaisuuksia siitä käyttää. Altiris-järjestelmän voi hankkia itselleen valitsemalla halutut ominaisuudet ja rakentamalla niistä toimivan kokonaisuuden. Erona kilpailijoihin on se, että Altiriksen mukana tulee myös oma ServiceDesk-ohjelmisto. [23.]

Novell Zenworks on kehuttu väline varsinkin ohjelmistojen toimittamiseen käyttöpäätteille. Kyseisestä ohjelmistosta löytyneen palautteen perusteella voisi päätellä, että kyseessä on erittäin kilpailukykyinen ohjelmisto. Sen osaajia on kuitenkin hankala löytää. Siitä löytää myös varsin vähän käyttäjien mielipiteitä aiheeseen liittyviltä palstoilta, mikä kertoo usein ohjelmiston vähäisestä suosiosta. [24.]

4.4.8 SQL-palvelin

Relaatiotietokannat ovat tietovarastoja, joissa eri tietojen välille on muodostettu yhteyksiä. Esimerkiksi taulukko asiakkaista voisi sisältää eri asiakkaat, niiden nimet, asuinpaikat, ikäluokan sekä tunnusnumeron. Tunnusnumeron avulla voidaan liittää

asiakas esimerkiksi listaan joka määrittelee kunkin tuotteen ostaneet asiakkaat. Uusia taulukoita voi luoda olemassa olevien taulukoiden tiedoilla SQL-kyselyillä. Mikäli haluttaisiin tietää, ketkä Helsigissä asuvat, ikäluokan 6 asiakkaat, ovat ostaneet tuotteen 1, 4, 5 tai 8, voisi asian selvittäminen käsin olla mahdottoman työlästä. SQL-palvelin voi selvittää asian tietokannan koosta ja palvelimen tehokkuudesta riippuen muutamassa sekunnissa. SQL-palvelin onkin välttämätön työkalu monille usein käytetyille järjestelmille. [25.]

Microsoft tarjoaa vuosittain uuden SQL Server julkaisun uusilla ominaisuuksilla. SQL Server on helppokäyttöinen, ja se sisältää lähes kaikki samat ominaisuudet kuin kilpailijansakin. Yritykselle, joka valitsee Windows-palvelimet, SQL Server on helppo valinta. Yritykselle, joka valitsee minkä tahansa muun kuin Windows-palvelimet, SQL Server ei ole vaihtoehto. SQL Server toimii ainoastaan Microsoftin tuotteiden kanssa, mikä heikentää sen asemaa yksittäisenä tuotteena. [26.]

Oracle on kallis, ja vaikeampi hallita kuin Microsoftin SQL Server. Se sisältää kuitenkin suurten tietokantojen hallintaan paremmat työkalut kuin Microsoftin SQL Server. Ehkä kuitenkin sen suurin etu SQL Serveriin on, että se toimii kaikilla alustoilla. Kun Linux-palvelimia on kuitenkin palvelimista suuri enemmistö, säilyttää Oracle myös asemansa hinnasta huolimatta. Se ei yleensä kuitenkaan ole järkevä ratkaisu Windows-palvelinverkkoihin hintansa vuoksi. [26.]

MySQL on suosittu ja ilmainen avoimen lähdekoodin ohjelmisto. Se tarjoaa ainoastaan tietokantapalvelimen perusominaisuudet vertailukelpoisella suorituskyvyllä. Se voi olla hyvä ratkaisu, mikäli tietokantapalvelimelta ei vaadita erityisiä ominaisuuksia. MySQL on yhteensopiva lähes kaikkien käyttöjärjestelmien kanssa. MySQL:n avulla pienempi yritys voi säästää kuluissa, mutta suuren yrityksen kannattaa yleensä sijoittaa johonkin enemmän ominaisuuksia ja mahdollisuuksia sisältävään tuotteeseen. [27.]

4.4.9 Tiedostopalvelin

Tiedostojen tallentaminen palvelimelle ei sinänsä vaadi mitään erityisiä asennuksia käyttöjärjestelmän lisäksi. Jaettavat kansiot pitää sijoittaa haluttuun paikkaan ja avata käyttäjille kansion ominaisuuksia muokkaamalla. Levytilaa pitää toki löytyä paljon ja riittävästi nopeutta, jotta käyttö ei hidastuisi jos useampi käyttäjä haluaa päästä käsiksi

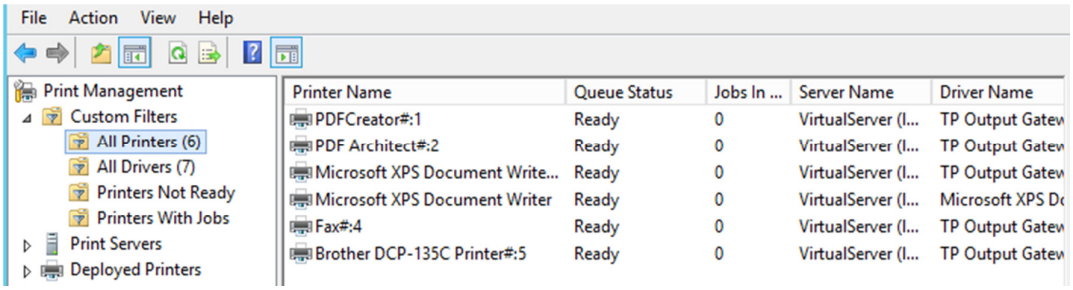
dataan samanaikaisesti. Tärkein varsinainen tehtävä tiedostopalvelimen asennuksessa on varmuuskopioinnin järjestäminen. Tallennettujen tietojen katoaminen laitevian takia ei saisi olla mahdollista.

Datan katoaminen yksittäisen levyn hajotessa pystytään estämään RAID-tekniikalla. Yleisimmin käytettyjä RAID-tasoja ovat 0, 1 ja 5. RAID 0 yhdistää useamman levyn yhdeksi suuremmaksi levyksi nopeuttaen tiedon hakua mutta ei luo varmuuskopioita eikä siten tarvitse ylimääräistä tallennustilaa. RAID 1 luo varmuuskopion levyn datasta toiselle levylle, haaskaten kuitenkin paljon levytilaa. RAID 5 jakaa datan vähintään kolmelle levylle suojaten datan yhden levyn rikkoutumiselta. RAID 5 luo tarkisteet jokaiselle datalohkolle, jotka vievät tilaa levyjen määrästä riippumatta yhden levyn verran. Tämä kuitenkin kuormittaa ohjainta enemmän, minkä takia RAID 5 ei ole niin tehokas kirjoittamaan kuin edellä mainitut tekniikat. Lisäksi kannattaa varmistaa levytilan määrän riittävyys ennen RAID 5:n käyttöönottoa. Uusia levyjä lisätessä täytyy kaikki levyt tyhjentää ennen RAID 5:n uudelleen asennusta. Uusia RAID-tekniikoita on kehitetty lukuisia edellä mainittujen pohjalta, yhdistäen näiden eri ominaisuuksia omalle järjestelmälle sopivasti. [28.]

4.4.10 Tulostinpalvelin

Tulostinpalvelin yhdistää verkkotulostimet toimialueen käyttäjiin. Se välittää palvelupyynnöt oikeille tulostimille ja tarkkailee tulostettavien dokumenttien liikennettä. Se myös välittää tulostimien ajurit niitä käyttäville koneille. Tulostinpalvelin on suoraan yhteydessä tulostimiin, joten usein ei ole tarpeellista sijoittaa paikalle varsinaista palvelinkonetta, vaan roolin voi ohjelmoida myös esimerkiksi reitittimeen.

Tulostinpalvelimen toiminta on parhaassa tapauksessa täysin automaattista. Se hakee siihen liitettyjen tulostimien ajurit ja välittää ne eteenpäin tietokoneille.



Kuva 9. Tulostinpalvelin on yksinkertainen järjestelmä.

Projektissa liitettiin isäntäkoneeseen Brothersoft-merkkinen tulostin, jota käytettiin kytkimellä isäntäkoneeseen liitetyllä kannettavalla. Roolin asennuksen jälkeen ei tarvinnut erikseen liittää tulostinta, vaan tulostin ilmestyi automaattisesti listaan.

4.4.11 VPN-palvelin

VPN välittää käyttäjälle yksityisen verkon palvelut julkisen verkon kautta. VPN voi yhdistää yksittäisen tietokoneen verkkoon tai yhdistää kaksi eri verkkoa toisiinsa. VPN antaa käyttäjälle mahdollisuuden työskentelyyn samoilla työkaluilla, kuin jos hän olisi suoraan kytkettynä verkkoon. VPN on monelle yritykselle pakollinen työkalu, mutta sen järjestäminen vaatii usein myös tietoturva järjestelyitä. Pelkkä verkon käyttäjätunnus ja salasana eivät aina riitä takaamaan riittävää turvaa.

DirectAccess on uusi vaihtoehto perinteiselle VPN:lle. Näiden kahden välillä suurin ero on, että DirectAccess Client on jatkuvasti päivitettävissä ja kontrolloitavissa. Tämän takia se muodostaa pienemmän tietoturvauhkan yritykselle. Käyttäjän luoma VPN-yhteys pitää kannettavan tietokoneen verkon valvonnassa niin kauan, kuin VPN-yhteys pidetään päällä, mutta muun ajan sen toimintaa ei pystytä kontrolloimaan. Esimerkiksi ryhmäkäytännöt ja virustorjunta eivät päivity tänä aikana. DirectAccess muodostaa kaksi eri yhteyttä, joista toinen on yhteydessä ainoastaan työasemien hallintatyökaluihin, ja toinen muodostaa VPN:n tavoin suoran yhteyden verkkoon. Mainituista yhteyksistä ensimmäinen on aina päällä, mikä antaa mahdollisuuden ryhmäkäytäntöjen ja virustorjunnan päivittämiseen aina koneen ollessa yhteydessä Internetiin. Toinen yhteyksistä voidaan muodostaa VPN:n tavoin erilaisia tunnisteita käyttämällä. DirectAccessin huono puoli on se, että se tukee ainoastaan IPv6 protokollaa, joka on uusin versio IP protokollasta. [29.]

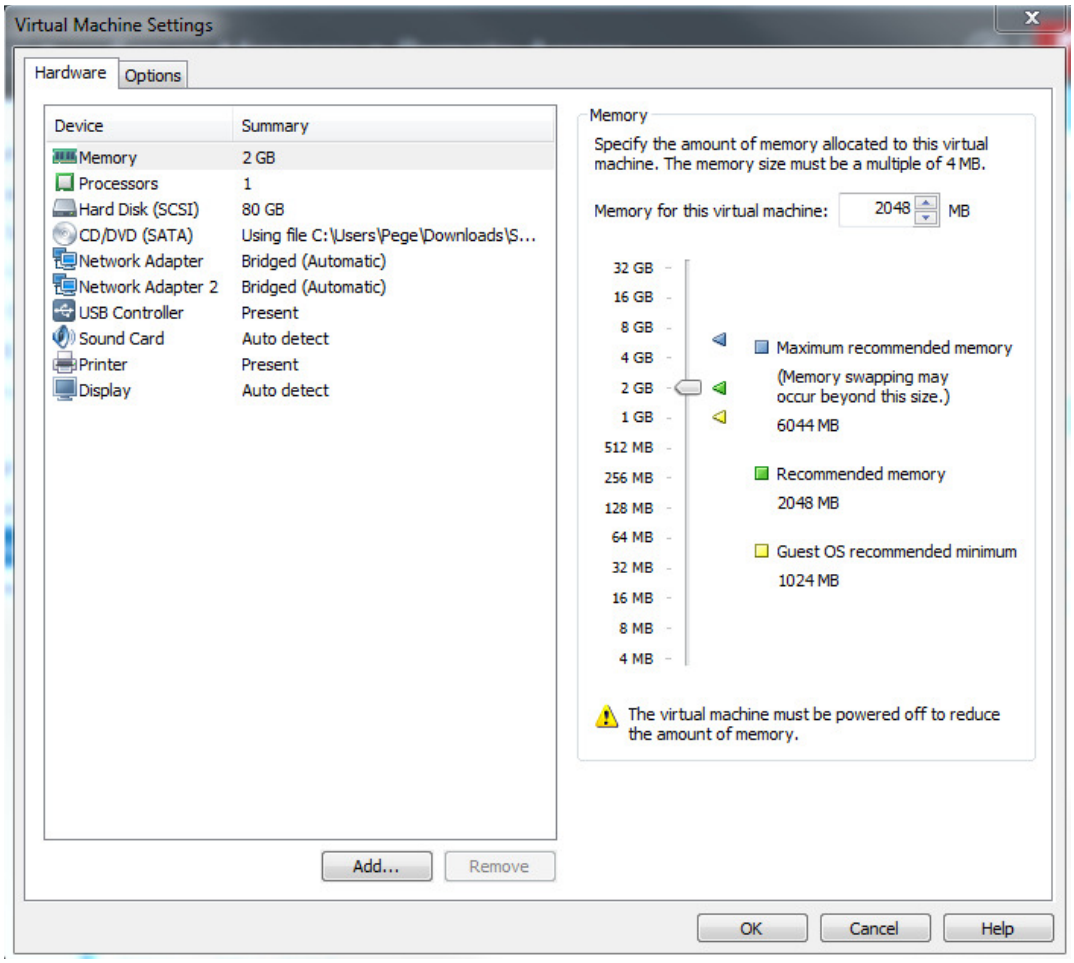
VPN-yhteys pitää luonnollisesti salata, mihin on useampia tapoja. Pelkkä käyttäjätunnuksen ja salasanan tunnistaminen ei välttämättä ole riittävä suojauskeino jos halutaan varmistaa, ettei kukaan tuntematon pääse verkkoon käsiksi, varsinkaan sen ulkopuolelta. Salaukseen voidaan käyttää esimerkiksi digitaalisia sertifikaatteja, datan kryptausta IP-securityllä tai yhteyden salausta Secure Shell (SSH) -suojauksella.

5 Verkon toteutus virtualisoidussa ympäristössä

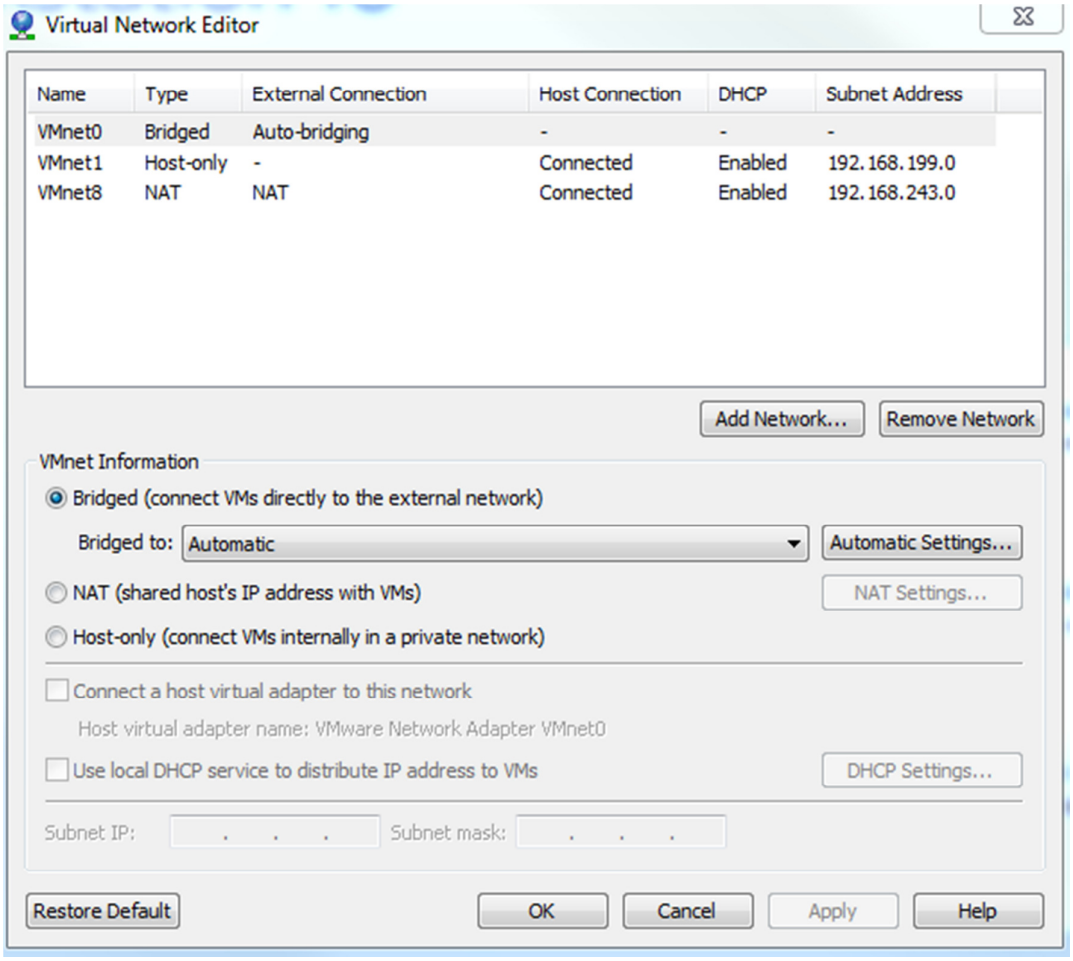
5.1 Verkon toteutus

Projekti suoritettiin kotioloissa joten varsinaisia laitteita ei kuulu lähiverkkoon kovin montaa. Isäntäkone on pienen kytkimen kautta yhteydessä kannettavaan tietokoneeseen sekä ISP:n reitittimeen, johon ei ole mahdollisuutta tehdä muutoksia.

Vaikka palvelinta käsitelläänkin isäntäkoneella, se on kuitenkin erillinen ja itsenäinen järjestelmä. Se ei ota automaattisesti käyttöön kaikkia isäntäkoneen fyysisiä ominaisuuksia. Virtuaalisella palvelimella ei ole esimerkiksi omaa verkkoporttia. Tämä on voinut joskus tuottaa paljon lisätyötä. Useimmissa virtualisointiohjelmissa tämä on kuitenkin saatu automatisoitua siten, että kaikki verkkoasetukset voi säätää ohjelman käyttöpaneelista. Kuvassa 9 esimerkkinä WMware Workstation 10:n näkymä. Tämä yksinkertaistaa verkon suunnittelua huomattavasti. Palvelinverkkoa suunnitellessa tulisi IP-verkko suunnitella huolellisesti ennen asennusta. Jokainen palvelin tarvitsee staattisen IP-osoitteen, sillä verkon eri laitteet kommunikoivat juuri tuon IP-osoitteen perusteella. Mikäli palvelin joudutaan käynnistämään uudelleen, saattaa sen IP-osoite muuttua, jolloin verkon muut palvelut eivät enää tunnista sitä. Palvelinten lisäksi pitää miettiä, kuinka paljon osoitteita DHCP-palvelin jaettavaksi muille laitteille.



Kuva 10. WMware Workstation 10 helpottaa virtuaalikoneen resurssien käyttöä.



Kuva 11. WMware:lla voidaan simuloida lähiverkko virtuaalikoneiden ja isäntäkoneen välille kolmella eri tavalla.

WMwaren Workstation 10 antaa mahdollisuuden luoda virtuaaliveron useammalla eri tavalla, jotka näkyvät kuvassa 11. Bridged-mallinen verkko tarkoittaa sitä, että palvelimet näyttävät ulospäin olevan osana isäntäkoneen lähiverkkoa. Niillä on omat IP-osoitteensa ja ne on kytkettynä virtuaalisen kytkimen kautta isäntäkoneen verkkosovittimeen. [30.]

Network Address Translation (NAT) antaa virtuaalikoneelle mahdollisuuden käyttää isäntäkoneen omaa IP-osoitetta. Se on usein helpoin tapa antaa virtuaalikoneelle yhteys verkkoon. Tässä tapauksessa palvelimet tarvitsevat kuitenkin oman IP-osoitteensa, joten vaihtoehto on pois suljettu. Tässä tapauksessa Wmware luo erillisen yksityisen verkon, jossa virtuaalinen DHCP-palvelin antaa virtuaalikoneelle osoitteen. Virtuaalinen NAT-laite ohjaa liikennettä ulkoisen ja sisäisen verkon välillä. [31.]

Host-only luo täysin erillisen verkon isäntäkoneen ja virtuaalikoneen välille. Tämä voisi olla hyödyllistä esimerkiksi palvelinverkon testauksessa, kun ei ole tarvetta muodostaa yhteyttä verkon ulkopuolelle. Tämän verkon voi kuitenkin myös liittää ulkoiseen verkkoon Windowsin verkkoadapterin avulla luotavalla silmukalla. [32.]

5.2 Verkon etähallintamahdollisuudet

Periaatteessa VPN-palvelin vaatii kaksi verkkoporttia käyttöönsä, joista toinen yhdistetään sisäverkkoon, ja toinen ISP:lle. Tämän voi kuitenkin suorittaa myös yhdellä verkkosovittimella antamalla sille molemmat roolit. VPN-palvelimella pitäisi olla staattinen IP-osoite, mutta ei DNS-palvelinta tai oletusyhdyskäytävää määriteltynä ISP:lle johtavassa verkkosovittimessa. Toimialueen verkkoon kytketyllä verkkosovittimella sen sijaan sekä IP-osoite että DNS-palvelin viittaavat suoraan toimialueeseen. Verkot tulisi nimetä selkeästi sekaannuksen välttämiseksi. [33.]

Verkon sisällä voidaan hallinnoida palvelimia etätyöpöytäyhteydellä. Tämä vaatii ainoastaan etäyhteyksien sallimisen palvelimelta sekä halutun käyttäjätunnuksen lisäämisen etäkäyttäjien ryhmään. Tämän jälkeen palvelinta voidaan hallinnoida miltä tahansa verkkoon liitetyltä koneelta oikeilla tunnuksilla Windowsin Remote Desktop Connection-työkalun avulla. Tämä käyttää Microsoftin kehittämää Remote Desktop Protocol (RDP) -protokollaa, missä RDP-asiakasohjelma ottaa yhteyttä RDP-palvelimeen. Sen asiakasohjelman asennus löytyy oletuksena lähes kaikista moderneista käyttöjärjestelmistä. Palvelimen asennus taas löytyy vakiona Windows-käyttöjärjestelmistä, mutta sen saa asennettua myös UNIX-pohjaisiin käyttöjärjestelmiin. [34.]

6 Käytännön toteutus

6.1 Projektin suunnittelu

Projektin tavoite oli itsenäisesti oppia olennaisia asioita Windows-palvelinympäristöistä ja virtuaalisoinnin tekniikoista, joten saatavilla olevista tekniikoista valittiin sen mukaan, minkä osaamisesta voisi olla hyötyä opintojen jälkeen. Lisäksi suunnitteluun vaikutti

ympäristö, jossa projekti toteutettiin. Isäntäkone, jossa oli asennettuna Windows 7, toimi paitsi alustana virtuaalipalvelimille, myös työkaluna dokumentoinnille ja tiedon etsinnälle. Tästä syystä käyttöjärjestelmän vaihtaminen esimerkiksi johonkin virtuaalisointiin erikoistuneeseen kevyeen käyttöjärjestelmään olisi voinut aiheuttaa hankaluuksia. Lisäksi mitään rahallista panostusta ei ollut tarkoitus lisätä projektin läpiviemiseen, joten kaikkien lisenssien tuli olla ilmaisia, tai muuten saatavilla olevia. Suurin osa maksullisista lisensseistä oli mahdollista hankkia ammattikorkeakoulu Metropolian kautta ilmaiseksi, ja tätä käytettiin hyväksi mahdollisimman paljon. Varsinkin WMwaren ja Microsoftin yrityskäyttöön tarkoitetut tuotteet olisivat olleet itse hankittuina tulevaisuudessa hintavia pelkkää oppimiskäyttöä ajatellen. Alussa oletettiin, että tietokoneen muisti riittäisi kaikkiin tehtäviin minimaalisella kuormituksella.

Palvelinten käyttöjärjestelmäksi valittiin Windows 2012 R2, koska sen käytön oppiminen kiinnosti. Tämän jälkeen tutkittiin ja verrattiin sen ominaisuuksia muihin vastaaviin ohjelmistoihin. Käyttöjärjestelmän lisäksi mietittiin mitä ominaisuuksia olisi tarkoitus ottaa käyttöön palvelinverkossa. Palvelimien roolien tulisi sisältää mahdollisimman paljon yleisesti yritysmaailmassa käytettyjä tekniikoita. Pääsääntöisesti päädyttiin yhteensopivuuksien takia Microsoftin tuotteisiin, mutta erityisesti MS Exchange mietitytti sen tarvitseman muistin määrän takia. Päädyttiin asentamaan Exchange ja valitsemaan lisäksi varalle toinen, vähemmän muistia tarvitseva, sähköpostipalvelin. Tämän lisäksi tarvittiin järjestelmänhallintaan oma työkalu, jonka rooliin valittiin Microsoftin System Center. Tutkiessani System Center-ohjelmistoa, huomasin sen vaativan tietokantapalvelimen toimiakseen. Tässäkin kohtaa päädyttiin Microsoftin tuotteeseen, eli SQL Serveriin.

Virtuaalikoneiden IP-verkon voi suunnitella monella eri tavalla, mutta tässä projektissa valittiin Bridged-mallinen verkko. Esimerkiksi sähköpostipalvelin vaatii toimiakseen yhteyden lähiverkon ulkopuolelle, mikä edellyttää palvelimelle omaa IP-osoitetta. Projektin ajaksi kaikille lähiverkon palvelimille sekä isäntäkoneelle annettiin staattinen, eli kiinteä IP-osoite, jotta mahdolliset muutokset osoitteissa eivät sekoittaisi palvelimien toimintaa.

6.2 Käytännön toteutus ja testaus

Isäntäkoneelle asennettiin ensin WMware Workstation 10, minkä jälkeen siihen lisättiin Windows Server 2012-levykuva ensimmäistä virtuaalipalvelinta varten. Käynnistyessään ensimmäistä kertaa palvelin ilmoitti välittömästi DC:n sekä AD:n tarpeesta, ja ohjasi pitkälle automatisoituun asennustyökaluun. Asennuksen aikana luotiin uusi toimialue ja toimialueen hakemisto. Tämän jälkeen lisättiin samaisella työkalulla tarvittavat roolit. Rooleja asennettaessa palvelin valitsi automaattisesti ominaisuudet ja muut roolit, joita tarvittiin valitun roolin toteuttamisessa. Mikäli joku vaadittu ominaisuus tai ohjelmisto ei löytynyt käyttöjärjestelmältä, ilmestyi ruudulle linkki, jonka takaa löytyi puuttuva ladattavana Microsoftin sivustolta. AD:n ja DC:n asennuksen jälkeen pystyttiin luomaan toimialueeseen konetilejä ja käyttäjiä, kirjautumaan toimialueeseen luoduilla käyttäjillä ja lähiverkkoon liitetyillä koneilla, käyttämään verkon palveluita sekä liittämään käyttäjiin erilaisia ryhmiä ja ryhmäkäytäntöjä.

Sähköpostipalvelinta varten luotiin uusi virtuaalipalvelin käyttämällä samaa menetelmää kuin edellisen palvelimen kohdalla. Varsinaisena erona asennuksessa oli, että virtuaalikone luotiin jo olemassa olevaan verkkoon, jolloin se liitettiin olemassa olevaan hakemistoon. Palvelinta ei myöskään asennettu DC:n rooliin. Palvelimelle asennettiin Exchange 2013 syöttämällä levykuva WMwaren virtuaaliseen DVD-asemaan. Ohjelman asennuksen jälkeen palvelin hidastui kuitenkin niin paljon, että se jouduttiin asentamaan uudelleen. Vaihtoehtoisesti asennettiin tilalle hMailServer. Itse sähköpostipalvelimen asennukseen löytyi selkeät ohjeet tuotteen sivustoilta, mutta sen toimintaan saattaminen olisi vaatinut ISP:n suostumuksen. Osa palveluntarjoajista ei oletusarvoisesti välitä dataa tarvittavan portin läpi.

SQL-palvelin luotiin järjestelmään System Centerin käyttöä varten. Sen asennusta varten suljettiin sähköpostipalvelin ja vapautettiin muistia uuden palvelimen luontiin. Alun perin asennettiin SQL Server 2014:n kanssa, mutta myöhemmin tilalle asennettiin SQL Server 2012 johtuen yhteensopivuus ongelmista System Centerin kanssa. SQL-palvelin vaati muutamia huomion arvoisia asetuksia. Suurin osa palveluista oli automaattisesti käynnistyviä ja SQL-palvelin käytti tässä projektissa Windows-tunnisteita. SQL-palvelin asetettiin kuuntelemaan ainoastaan staattisia portteja, sillä se luotiin ainoastaan System Centeriä varten, eikä järjestelmän IP-osoitteiden ollut tarkoitus muut-

tua missään tilanteessa. SQL-palvelin vaati lisäksi omat järjestelmänvalvojan käyttäjätunnuksensa palveluiden käynnistämiseen.

System Centerillä pyrittiin hallitsemaan toimialueeseen liitettyä kannettavaa tietokonetta. Aikaisemmin System Centeriä varten luotiin SQL-palvelin samalle virtuaalikoneelle. SQL-palvelimen lisäksi System Center vaati toimiakseen IIS:n sekä useita ohjelmistopäivityksiä. System Center saatiin yhteyteen verkkoon liitetyn kannettavan tietokoneen kanssa. Lähellekään kaikkia toimintoja ei saatu toimimaan, mutta System Center on niin laaja kokonaisuus, ettei sen kaikkia ominaisuuksia nähty tarpeelliseksi toteuttaa.

VPN-palvelin luotiin viimeisenä, sillä sen nähtiin aiheuttavan eniten muutoksia verkkoympäristöön, ja siten olevan haastavin osa projektia. Lisäksi usein ongelmia ratkoessa poistettiin palomuuri käytöstä, mikä olisi voinut saastuttaa virtuaalisen verkon VPN:n ollessa toiminnassa. Myös tietoturva ominaisuudet luotiin vain täyttämään minimi vaatimukset. Palvelimelle asennettiin sekä VPN että DirectAccess. Ensimmäisenä toimenpiteenä asennettiin tarvittavat roolit ja ominaisuudet palvelimelle. Tämän jälkeen luotiin uusi virtuaalinen verkkoportti VPN-yhteyttä varten. Portille ei määritelty oletusyhdyskäytävää, ja se luotiin eri verkkoon, kuin muut palvelimet virtuaaliverkossa. VPN-yhteys ei missään vaiheessa toiminut täydellisesti, mutta yhteys saatiin kuitenkin muodostettua ajoittain.

7 Yhteenveto

Lopputuloksen perusteella voidaan sanoa, että pieniä poikkeuksia lukuun ottamatta, palvelinverkon rakentaminen on yllättävän helppoa uusilla järjestelmillä. Lähes kaikki asennukset on automatisoitu ja ohjeistus asennuksen epäonnistuessa auttaa paljon. Toki erilaisten valintojen tekeminen vaatii edelleen tietoa aiheesta, mutta oletusarvoja käyttämällä pääsee asennuksen lähes aina loppuun asti. Käyttöympäristö asetti tässä projektissa omat rajoitteensa, jotka haittasivat etenkin sähköpostipalvelimen toimintaa. Isäntäkoneen muisti ei käytetyllä kokoonpanolla tapauksessa riittänyt ylläpitämään muita käyttöjärjestelmiä ja ohjelmistoja Exchangen rinnalla, mikä olisi yksinäänkin vaatinut sujuvaan toimintaan kaiken tarjolla olleen muistin. Eri roolien kuormittaminen

eri aikaan auttoi muissa tapauksissa.

Eri rooleista VPN vaatii selvästi eniten pohdiskelua. Muista rooleista poiketen se tarjoaa useita vaihtoehtoja sen sijaan, että ehdottaisi selkeää ja toimivaa ratkaisua tilanteeseen. Virtuaalikoneiden kytkeytyminen lähiverkossa, salauksen käyttö ja digitaalisten varmenteiden luominen tuottivat haasteita. Myös Exchangen asetukset vaativat hieman opiskelua. Oikeastaan kaikki roolit ja ohjelmistot, jotka ottivat yhteyttä sisäverkon ulkopuolelle, vaativat tietämystä. Tämä on tietenkin luonnollista, koska ulkoiset tekijät muuttuvat paljon eri verkkoihin vaihdettaessa, eikä niiden yhteyteen pysty rakentamaan mitään yleisesti pätevää ohjesääntöä. Kuitenkin pienellä ohjeistamisella pystyttäisiin viemään käyttöjärjestelmässä selkeästi tavoiteltua helppokäyttöisyyttä vielä nykyistä pidemmälle.

Virtuaalisoinnin lisääminen projektiin WMwarella ei juuri vaikeuttanut asioita, vaikka fyysisten laitteiden lisääminen olisi joissakin tilanteissa selkeyttänyt kokoonpanoa. Tämän sijaan virtuaalisointi antoi joustavuutta varsinkin resurssien jakamiseen verkon eri palvelinten kesken. Tällä tavalla pystyin myös kokeilemaan esimerkiksi sähköpostipalvelimen asennusta, vaikka alkuun tiedettiin että se tulee kuormittamaan konetta liikaa. Kun palvelin ei asennuksen jälkeen enää reagoinut käskyihin hitautensa takia, pystyi sen huoletta poistamaan WMwaresta. Tilalle sai helposti luotua uuden palvelimen ja vanhan sai poistaa isäntäkoneelta viemästä ylimääräistä levytilaa. WMware antoi myös useita mahdollisuuksia sisäverkon toteutukseen, joskin tätä ominaisuutta tullaan varmasti kehittämään paljon monipuolisemmaksi tulevaisuudessa. Kaiken kaikkiaan WMwarella saa aikaan ihanteellisen testiympäristön, jolla on helppo toteuttaa ja suunnitella palvelinverkko ennen sen toteuttamista käytännössä.

Kaiken kaikkiaan Microsoft suosii niitä, jotka käyttävät pelkkiä Microsoftin tuotteita. Windows ympäristön helppokäyttöisyys yhdistettynä hyvään suorituskykyyn vetoaa suurimpaan osaan käyttäjistä. Lisäksi Microsoftin tuotteet on suunniteltu toimimaan nimenomaan toistensa kanssa. Vaikka muiden valmistajien ohjelmistoilla saisikin aikaan säästöjä, ei se välttämättä ole kannattavaa jos työtunteja asennuksessa kertyy liikaa, tai ongelmia esiintyy liian usein. Palvelinverkkoa suunnitellessa on muutenkin helpompaa valita yksi tuotemerkki, sillä tukea on vaikea saada jos jotain menee vikaan yhdistäessä kahta erilaista järjestelmää. Tämä pätee varsinkin jos toinen mainituista on Microsoftin järjestelmä.

Tavoitteena projektissa oli ennen kaikkea oppia uusia asioita palvelinympäristön luomisesta ja toiminnasta. Lisäksi tavoitteena oli saada verkko näyttämään ulospäin pienen yrityksen palvelinverkolta. Ensimmäisessä tavoitteessa onnistuttiin, mutta toissijainen tavoite jäi saavuttamatta. Tämä johtuu osittain muistin riittämättömyydestä varsinkin Exchangen kohdalla.

Lähteet

1 Mäntylä, Juha-Matti. 2008. Verkkodokumentti. Tietoviikko. 30.11.2008 <http://www.tietoviikko.fi/cio/virtualisointi+mullistaa+tietotekniikan/a192316>. Luettu 1.4.2014.

2 Desktop Virtualization. Verkkodokumentti. Wikipedia. <en.wikipedia.org/wiki/Desktop_Virtualization>. Päivitetty 13.5.2014. Luettu 1.4.2014.

3 App virtualization. Verkkodokumentti. SearchVirtualDesktop. <http://searchvirtualdesktop.techtarget.com/definition/app-virtualization>. Päivitetty 1.11.2011. Luettu 1.4.2014.

4 Local area network. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Local_area_network>. Päivitetty 8.5.2014. Luettu 1.4.2014.

5 Wide area network. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Wide_area_network>. Päivitetty 19.5.2014. Luettu 1.4.2014.

6 Johdanto verkkotekniikkaan. Verkkodokumentti. <http://www.okol.org/verkkokurssit/datanomi/tietojarjestelmien_kaytto_ja_kehittami-nen/lahiverkko_internet/lanjaint/johdanto_verkkotekniikkaan/johdanto2.htm>. Päivitetty 12.2.2004. Luettu 1.4.2014.

7 Dell PowerEdge VTRX review. Verkkodokumentti. Zdnet. <http://www.zdnet.com/dell-poweredge-vrtx-review-a-versatile-server-storage-and-networking-package-7000025930>. Päivitetty 4.2.2014. Luettu 1.4.2014.

8 Mail server role: Configuring a mail server. Verkkodokumentti. Microsoft. <http://technet.microsoft.com/en-us/library/cc780996(v=ws.10).aspx>. Päivitetty 21.1.2005. Luettu 1.4.2014.

9 vSphere ESXi Hypervisor. Verkkodokumentti. WMware. <https://www.vmware.com/products/vsphere/features/esxi-hypervisor.html>. Luettu 1.4.2014.

10 Lam, William. Running ESXi 5.5/5.5u1 on Apple Mac Mini + Thunderbolt Ethernet Adapter Caveat. Verkkodokumentti. virtuallyGhetto. <http://www.virtuallyghetto.com/2013/09/running-esxi-55-on-apple-mac-mini.html>. Päivitetty 9.3.2013. Luettu 1.4.2014.

11 Red Hat Enterprise Virtualization. Verkkodokumentti. Red Hat. <http://www.redhat.com/products/cloud-computing/virtualization>. Luettu 1.4.2014.

12 User reviews for Citrix XenServer. SpiceWorks. <http://community.spiceworks.com/product/19260-citrix-xenserver>. Luettu 1.4.2014.

13 Domain controllers. Verkkodokumentti. Microsoft. <http://technet.microsoft.com/en-us/library/cc977987.aspx>. Luettu 1.4.2014.

14 DNS. Verkkodokumentti. Microsoft. <http://technet.microsoft.com/en-us/library/cc730921.aspx>. Luettu 1.4.2014.

15 DHCP Server. Verkkodokumentti. Microsoft. <http://technet.microsoft.com/en-us/windowsserver/dd448608.aspx>. Luettu 1.4.2014.

16 Active Directory. Verkkodokumentti. Microsoft. <http://technet.microsoft.com/en-us/library/bb742424.aspx>. Luettu 1.4.2014.

17 PowerShell. Verkkodokumentti. Microsoft. <http://technet.microsoft.com/en-us/library/ff950685.aspx>. Päivitetty 17.4.2012. Luettu 1.4.2014.

18 Some useful PowerShell scripts. Keskustelupalsta. Cert Collection. <http://certcollection.org/forum/topic/108555-some-useful-powershell-sample-scripts>. Päivitetty 23.4.2011. Luettu 1.4.2014.

19 Create and Edit a Group Policy Object. Verkkodokumentti. Microsoft. <http://technet.microsoft.com/en-us/library/cc754740.aspx>. Päivitetty 17.4.2012. Luettu 1.4.2014.

20 Checklist: Perform a New Installation of Exchange 2013. Verkkodokumentti. Microsoft. <http://technet.microsoft.com/en-us/library/ff805042(v=exchg.150).aspx>. Päivitetty 28.1.2014. Luettu 1.4.2014.

21 Configure Mail Flow and Client Access. Verkkodokumentti. Microsoft. <http://technet.microsoft.com/en-us/library/4acc7f2a-93ce-468c-9ace-d5f7eecbd8d4(v=exchg.150)#CreateConnector>. Päivitetty 20.3.2013. Luettu 1.4.2014.

22 Internet Information Services. Verkkodokumentti. Microsoft. <http://technet.microsoft.com/en-us/library/bb124674(v=EXCHG.65).aspx>. Päivitetty 23.5.2005. Luettu 1.4.2014.

23 Endpoint Management powered by Altiris Technology. Verkkodokumentti. Symantec. <http://www.symantec.com/endpoint-management>. Luettu 1.4.2014.

24 ZENworks 11 SP3 Brings IT. Verkkodokumentti. Novell. <http://www.novell.com/products/zenworks/endpoint-management/#Learn>. Luettu 1.4.2014.

25 SQL. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/SQL>. Päivitetty 13.5.2014. Luettu 1.4.2014.

26 Stansfield, Josh. Microsoft SQL Server vs. Oracle: The Same But Different? Verkkoblogi. Segue Technologies. <http://www.seguetech.com/blog/2014/03/13/Microsoft-SQL-Server-versus-oracle>. Päivitetty 13.3.2014. Luettu 1.4.2014.

27 Ehinger, Benjamin. MySQL vs Oracle. Verkkodokumentti. ITX Design. <http://itxdesign.com/mysql-vs-oracle> Päivitetty 21.2.2014. Luettu 1.4.2014.

28 RAID. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Redundant_array_of_independent_disks>. Päivitetty 28.5.2014. Luettu 1.4.2014.

29 Shinder, Deb. DirectAccess versus VPN: They are Not the Same. Verkkodokumentti. WindowsSecurity.com. <http://www.windowsecurity.com/articles-tutorials/misc_network_security/DirectAccess-versus-VPN-They-Not-Same.html>. Päivitetty 8.9.2010. Luettu 1.4.2014.

30 WMware Workstation 4. Verkkodokumentti. WMware. <https://www.vmware.com/support/ws4/doc/network_bridged_ws.html>. Luettu 1.4.2014.

31 WMware Workstation 4. Verkkodokumentti. WMware. <https://www.vmware.com/support/ws4/doc/network_nat_ws.html>. Luettu 1.4.2014.

32 WMware Workstation 4. Verkkodokumentti. WMware. <https://www.vmware.com/support/ws4/doc/network_host_ws.html>. Luettu 1.4.2014.

33 Configure a Remote Access VPN Server. Verkkodokumentti. Microsoft. <http://technet.microsoft.com/en-us/library/cc725734(v=ws.10).aspx>. Luettu 1.4.2014.

34 Configuring Remote Desktop. Verkkodokumentti. Microsoft. <http://technet.microsoft.com/en-us/library/bb457106.aspx>. Luettu 1.4.20143.11.2005

35 Comparison of platform virtualization software. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Comparison_of_platform_virtualization_software>. Päivitetty 27.5.2014. Luettu 1.4.2014.

36 Mayer, Keith. WMware or Microsoft? Comparing vSphere 5.5 and Windows Server 2012 R2 Hyper-V At-A-Glance. Verkkoblogi. keithmayer.com. <http://blogs.technet.com/b/keithmayer/archive/2013/09/24/vmware-or-microsoft-comparing-vsphere-5-5-and-windows-server-2012-r2-at-a-glance.aspx>. Päivitetty 15.10.2013. Luettu 1.4.2014.

37 XenServer Configuration Limits. Verkkodokumentti. Citrix. <http://support.citrix.com/servlet/KbServlet/download/34966-102-704363/CTX137837_XenServer%206_2_0_Configuration%20Limits.pdf>. Luettu 1.4.2014.

38 SUSE Linux Enterprise Server Virtualization with KVM. Verkkodokumentti. openSUSE. <http://doc.opensuse.org/products/draft/SLES/SLES-kvm_sd_draft/cha.kvm.limits.html>. Päivitetty 25.6.2012. Luettu 1.4.2014.